Gestion de l'interférence dans les réseaux à diffusion : incertitude du canal et contraintes de sécurité.

Meryem Benammar

N° d'ordre : 2014-26-TH

SUPELEC

ECOLE DOCTORALE STITS
« Sciences et Technologies de l'Information des Télécommunications et des Systèmes »

THÈSE DE DOCTORAT

DOMAINE : STIC
Spécialité : Télécommunications

Soutenue le
15 Décembre 2014

par:

Meryem BENAMMAR

Gestion de l'interférence dans les réseaux à diffusion: incertitude du canal et contraintes de sécurité

Interference Management in Broadcast Networks: Channel Uncertainty and Security Constraints

Membres du Jury :

Gerhard KRAMER	Technische Universität München	Rapporteur
Gerald MATZ	Technische Universität Wien	Rapporteur
Mérouane DEBBAH	SUPELEC, chaire Alcatel Lucent	Examinateur
Pierre DUHAMEL	LSS-SUPELEC, Division Télécoms et réseaux	Examinateur
Pablo PIANTANIDA	SUPELEC (encadrant de thèse)	Examinateur
Hikmet SARI	SUPELEC (directeur de these)	Invité
Michèle WIGGER	Telecom ParisTech	Examinateur

Remerciements

Au terme d'un travail de longue haleine il est temps pour moi, Dieu Merci, de me tourner vers toutes les personnes qui m'ont soutenue ces trois années durant et de leur adresser mes sincères et profonds remerciements.

Cette thèse a vu le jour au sein du département des Télécommunications de Supélec, un beau jour d'Octobre 2011, et a duré trois années sous l'excellent et valeureux encadrement de Prof. Pablo Piantanida. Pablo qui a toujours su trouver les bons mots pour m'encourager, Pablo avec qui nous avons passé des heures au tableau tentant d'apprivoiser tel théorème ou telle autre preuve saugrenue, Pablo avec qui nous avons partagé les grandes joies des résultats de capacité mais aussi les petites déconvenues mathématiques, et j'en passe ... Pablo a mes éternels gratitude et respect.

Ensuite, pour m'avoir fait l'honneur de lire et commenter mon manuscrit de thèse et pour m'avoir gratifiée de leur présence à ma soutenance de thèse, je tiens tout particulièrement à remercier mes deux rapporteurs les Professeurs Gerald MATZ et Gerhard KRAMER. Je tiens aussi à remercier très chaleureusement les membres de mon jury de thèse pour leur présence et leur participation à ma soutenance, allant des remarques pertinentes de Prof. Michèle WIGGER aux questions judicieuses de Prof. Mérouane DEBBAH, passant par les commentaires instructifs de Prof. Hikmet SARI et finissant par les conseils inestimables de Prof. Pierre DUHAMEL.

Je dois une fière chandelle aussi à mes parents dont le soutien a toujours été constant et inconditionnel durant toutes ces années. J'espère leur avoir rendu en fierté ce que eux m'ont donné en sacrifice et amour dévoué et je sais que ce n'est que maigre récompense pour tous leurs efforts passés.

A mes adorables collègues, je dois aussi des remerciements plus que chaleureux. Mes chers collègues de bureau et de département: German, Chao, Cheng-Chiun, Farhane et kiran, Abdulaziz et Shirin, Dora, Bakarime, Matha, Kenza et Azary, mes collèges du L2S et d'autres laboratoires d'E3S: Assia, Leila, Jinane, Amina, Safae, Bouthaina, Jad, Mahmoud, Mohamad et Iyad, font sans doute partie des personnes qui ont le plus égayé mes jours au A4.19 à Supélec et je les en remercie de tout mon coeur. Aussi, souhaiterais-je remercier mes anciens collègues de bureau: Joffrey, Amr, Ayaz, Najett et Marina, qui m'ont initiée au travail de thèse et ont été de conseils bien plus que valeureux pendant mes premiers mois de thèse. Et au final, je souhaite remercier du fond du coeur mes collègues et amis avec qui il m'a été donné de lancer l'association des doctorants ADSS et qui ont mené au mieux cette expérience humaine hors du commun: Matthieu, Elsa, Pierre, Maud, Najett et Ashish.

Comment citer le couloir A4 sans citer Catherine, l'ange gardien des doctorants à qui nous devons tous une fière chandelle, ou encore Vuong et ses grandes discussions politico-socio-économique ou encore José, l'homme du département au grand coeur? Comment oublier aussi tous le corps enseignant du département des télécommunications: Mari, Sheng, Mr Sari, Mohamad, Jocelyn ... et plus particulièrement Messieurs Dumas et Barreau qui m'ont toujours suivie et encouragée pendant ma thèse?

Je ne pourrais pas non plus oublier de citer tous les professeurs et corps administratif de Supélec avec qui j'ai eu le plaisir d'échanger, de discuter et de partager des moments inoubliables tels que Mme VAN DEN TORREN qui m'a été d'une aide inestimable pour

ma recherche d'emploi, ou encore Philippe BALVOIRAT (PhiPhi) sans qui le sport à Supélec serait dépourvu de toute âme, ou encore Véronique BERNAS qui oeuvre dans l'ombre pour le centre de documentation, Bich-Lien DOAN à qui les doctorants doivent tant et de nombreuses autres personnes qui ont à un moment ou un autre été déterminantes dans mes choix et cursus (Hana BAILI, Gaelle LAHOUN). Je les remercie tout un chacun pour leur bon conseil et soutien inconditionnel.

A mes amis aussi je dédie mes remerciements les plus sincères, eux qui ont toujours été à mes côtés et qui le sont toujours depuis plusieurs années maintenant, et pour le restant de la vie je l'espère. A mes amis: Asmae, Abir, Omar, Arij, Camille, Pascaline, Ghada, Ibtihal, Dina, Fatima-Zohra, Ahmed, Claire, et j'en oublie très certainement plus je n'en cite, à mes amis, je dois beaucoup de courage et de persévérance.

Avant de conclure, je remercie toute ma famille au Maroc qui a toujours cru en moi et qui ne cesse de me signifier fierté et orgueil, j'espère qu'ils sauront combien leurs encouragements ont été valeureux et que malgré les distances, leurs pensées me parviennent toutes.

Au final, mon plus grand merci ira sans doute à ma jumelle, Bouchra, sans qui mon existence n'aurait point de sens. Les mots failliront à décrire ce qu'elle a été et ce qu'elle sera toujours pour moi, et pour cela, je ne trouve point à rajouter que de lui dédier tous mes travaux de thèse.

A Bouchra, mon Autre.

Contents

State Of Publications

Journal papers

- M. Benammar, P. Piantanida, and S. Shamai (Shitz). "Capacity results for some classes of Multicast Cognitive Interference Channel". *in preparation for submission to IEEE Trans. on Information Theory*, 2014.
- M. Benammar and P. Piantanida, and S. Shamai (Shitz). "On the Compound Broadcast Channel: The role of Multiple Description coding and Interference Decoding". *submitted to IEEE Trans. on Information Theory*, Available on-line: http://arxiv.org/abs/1410.5187
- M. Benammar and P. Piantanida. "On the secrecy capacity region of the Wiretap Broadcast Channel". *submitted to IEEE Trans. on Information Theory*, Available on-line: http://arxiv.org/abs/1407.5572

Conference papers

- M. Benammar, P. Piantanida, and S. Shamai (Shitz). "Capacity results for some classes of Multicast Cognitive Interference Channel". *IEEE Information Theory Workshop 2015, Jerusalem.*
- M. Benammar, P. Piantanida. "The secrecy capacity region of a class of Parallel Wiretap Broadcast Channels". In *52nd Annual Allerton Conference on Communication, Control, and Computing*, 2014.
- M. Benammar and P. Piantanida. "On the secrecy capacity region of the Wiretap Broadcast Channel". In *IEEE Information Theory Workshop (ITW)*, Nov 1 – 5 , 2014 (Hobart, Tasmania).
- M. Benammar, P. Piantanida, and S. Shamai (Shitz). "Multiple Description coding for the Compound Broadcast Channel". In *IEEE Information Theory Workshop (ITW)*, Nov 1 – 5 , 2014 (Hobart, Tasmania).
- M. Benammar, P. Piantanida, and S. Shamai (Shitz). "Dirty-paper coding techniques for compound MISO Broadcast Channels: a DoF analysis". In *Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM), 2014 9th International Conference on*, pages 442–447, 2014.
- M. Benammar, P. Piantanida. "On the role of Interference Decoding in Compound Broadcast Channels". In *IEEE Information Theory Workshop (ITW), 2013.*

List of Figures

Résumé étendu en Français

Introduction

Du fait que les télécommunications ont connu un essor des plus considérables lors de la dernière décennie, et dans la perspective de créer pour chaque utilisateur un environnement totalement connecté, les réseaux actuels et futurs doivent s'adapter à cette tendance sur les deux plans du trafic supporté et de l'architecture réseaux.

D'une part, les systèmes de communication futurs sont amenés à véhiculer un trafic réseau en constante évolution (flux de voix et de vidéos, signaux de commande en temps réel, trafic à faible débit, ...). Chaque type de trafic, de par l'application à laquelle il est destiné, doit répondre à un ou plusieurs critères dont: un haut débit (application vidéos), faible latence (signaux de sécurité), haute fiabilité (signaux de commande), intégrité et confidentialité (sécurité)...

D'autre part, afin de transporter un trafic aussi hétérogène à travers le réseau, l'archi--tecture doit être aussi en rupture avec les architectures traditionnelles en station de base et user terminaux. L'architecture optimale reste encore à définir, ceci dit elle passera certainement par une multiplication des points d'accès au réseau. Cette multiplication peut se faire en permettant à plusieurs composants du réseau de jouer le rôle de transmetteur ce qui a pour effet d'augmenter les débits et puissances disponibles et de fournir un meilleur accès à l'information. Par conséquent, plusieurs scénario de communication sont amenés à coexister au sein du même réseau citant par exemple la diffusion (Broadcast), la transmission simultanée (Multicast), le relai (Relay) ou encore les scénarios cognitifs à interférences (Conginitive interference) etc.

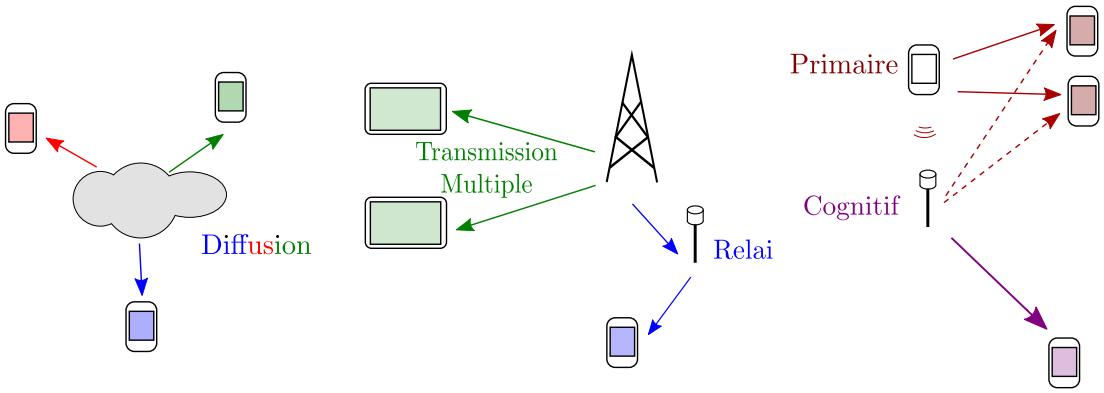


Figure 1: Scénarios de communication de base

1 Problématiques et principaux modèles de canaux

Au regard de la nature ouverte des transmissions sans fil, l'augmentation des noeuds à l'émission et à la réception résulte en des interférences fortes et non-structurées, et ce au sein du même environnement de communication ainsi qu'au niveau des systèmes de communication adjacents.

La gestion d'interférences étant l'élément le plus limitant dans les transmissions sans fil, les stratégies de gestion d'interférences sont d'un attrait particulier bien qu'elles restent encore méconnues pour bien des classes de canaux. L'un des canaux pour lesquels il est crucial de développer des stratégies efficaces de gestion d'interférences, ne serait-ce que pour le cas de deux utilisateurs, est sans doute le canal à diffusion [1]. D'un point de vue de théorie de l'information, un canal à diffusion consiste en une source désirant transmettre deux messages distincts, chacun à un utilisateur, sans erreur. Pour ce, la source est tentée de transmettre les messages chacun à son débit maximal, ceci dit, l'augmentation du débit d'un message résulte en une augmentation de l'interférence à l'utilisateur opposé. C'est la résolution de ce compromis qu'on dénote par gestion de l'interférence.

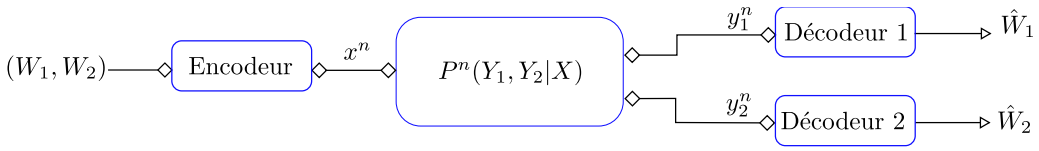


Figure 2: Canal de diffusion standard

En plus d'être vulnérables à l'augmentation des interférences, les communication sans-fil sont aussi assujetties à des qualités de lien variables, une variabilité qui, à elle seule, peut être critique pour les applications sensibles à la fiabilité ou latence des données (signaux de sécurité, signaux de commande dans les centrales électriques, etc). Couplée à cette incertitude du canal, l'interférence devient de plus en plus critique d'où la nécessité d'établir des techniques de gestion d'interférence qui soient robustes à l'incertitude canal.

Canal de diffusion avec incertitude

L'information canal (gain, niveau de bruit, matrice de transition du canal, etc) étant modélisée par une variable d'état, la disponibilité de cette information à la source et sa variabilité définissent différentes classes de canaux à incertitude: canaux composés, canaux composites, canaux à variation temporelle arbitraire ... Dans cette thèse, nous intéressons aux canaux de diffusion à incertitude composés où l'état est supposé inconnu à la source mais constant dans le temps. Dans de tels scénarios, la source ignore la réelle distribution de probabilité contrôlant le canal mais connaît un ensemble de lois auquel elle peut appartenir. Ce genre de canaux est un modèle approprié pour les canaux à évanescence lente où le gain des canaux est supposé varier sur une durée bien supérieure à la durée de la transmission. La gestion d'interférences dans de tels canaux s'avère davantage complexe de par cette incertitude et a donc fait l'objet d'une étude approfondie dans cette thèse.

Transmissions multiples sur les canaux à interférences cognitifs Rappelons que lorsque la source ignore laquelle parmi un ensemble de lois est celle qui régit la transmission de l'information, elle est contrainte à transmettre simultanément à toutes

les lois ainsi qu'elle aurait transmis à plusieurs utilisateurs simultanément. Les canaux à incertitude sont donc souvent assimilés aux canaux à transmissions multiples où plusieurs utilisateurs souhaitent décoder le même message. Dans cette thèse, nous étudions par là même une classe de canaux limités par les interférences, les canaux à interférences cognitifs, lorsque ceux là sont sujets aux transmissions multiples. De tels canaux consistent en deux sources transmettant chacune à un utilisateur distinct, mais dont l'une (source cognitive) connaît à priori le message que l'autre source (source primaire) transmet.

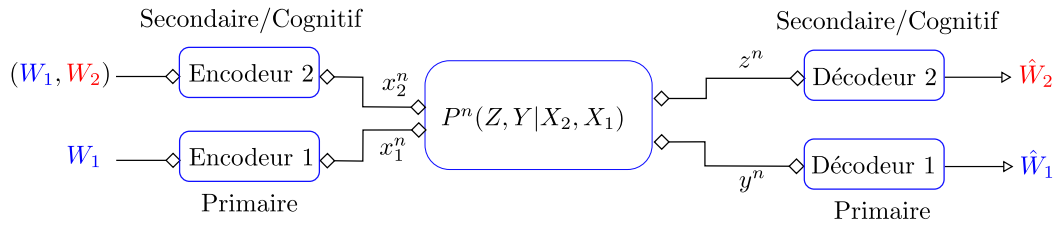


Figure 3: Le canal cognitif à interférence

Bien que ce canal soit assez similaire au canal à interférences, il doit à plus juste titre être considéré comme un canal de diffusion avec noeud auxiliaire. Lorsque ce noeud, source primaire, aide à la transmission du message primaire W_1 il crée de l'interférence pour l'utilisateur opposé qui ne souhaite décoder que le message secondaire W_2, un compromis doit être trouvé entre les deux débits transmis. En présence de transmissions multiples, ce compromis s'avère d'autant plus nécessaire que la source doit satisfaire la demande de plusieurs utilisateurs simultanément. Des scénarios de communication similaires peuvent intervenir dans les grands stades sportifs où un signal commun à tous les supporteurs est transmis sur leur équipement de réception (replay, statistiques ...) et où une station de base voisine aide à la transmission de ce signal tout en assurant la couverture d'autres utilisateurs du réseau. Notre but dans cette thèse est de développer les schémas optimaux de codage pour de tels canaux surtout en la matière de gestion de l'interférence.

Le canal de diffusion avec espion: De par la nature ouverte des communications sans fil, la multiplication des points d'accès au réseau impacte notablement la sécurité de l'information au niveau de la couche physique. La sécurité au niveau de couche physique désigne toutes les techniques de sécurisation de données sans recourir au cryptage de l'information aux couches supérieures de la pile des protocoles de transmission. En pratique, une communication peut être affectée par deux types d'espionnage. Un espionnage actif où le noeud espion altère l'information (noeud parasite) et un espionnage passif où l'espion accède à une information qu'il n'est pas sensé obtenir (accès à un service pour les membres non abonnés). Afin qu'une communication soit sécurisée, les débits transmis se doivent d'être assez faibles pour être correctement décodés aux utilisateurs légitimes mais aussi assez élevés pour ne pas être décodés par le noeud espion. Ce compromis est modélisé théoriquement par le canal à espion [2] où une source cherche à transmettre un message à un utilisateur légitime tout en le sécurisant par rapport à un espion externe. La sécurisation de données au niveau de la couche physique présente l'avantage d'être robuste aux algorithmes de craquage de force brute, et a donc un attrait tout particulier lorsque le noeud espion a une grande capacité calculatoire. Ceci dit, elle repose essentiellement sur les propriétés statistiques des canaux des noeuds et s'avère impossible lorsque le canal

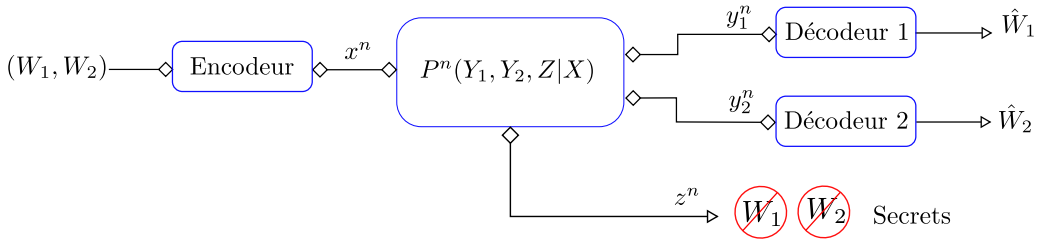


Figure 4: Le canal de diffusion à espion

de l'espion est de meilleure qualité que celui de l'utilisateur légitime. Dans cette thèse, nous nous intéressons à la classe de canaux qui combinent sécurité et diffusion: canaux de diffusion avec espion.

Dans ce qui suit, nous introduisons de manière succincte et détaillée les trois grandes problématiques de ces travaux de thèse.

2 Le canal de diffusion à incertitude

Considérons le canal diffusion suivant où une source cherche à transmettre deux messages (W_1, W_2) à deux utilisateurs Y and Z Fig. 5 dont les canaux peuvent être régis respectivement par M ou N lois de probabilité.

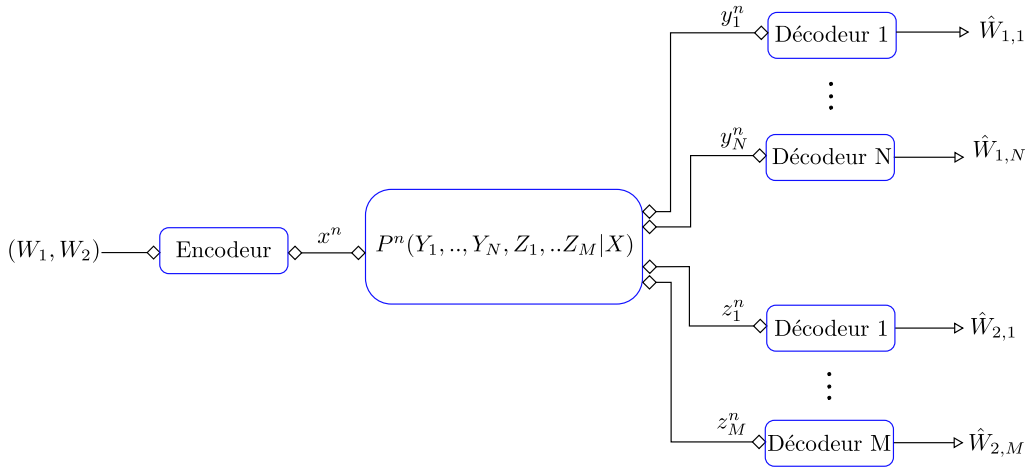


Figure 5: Le canal de diffusion à incertitude N par M.

Tels que nous l'avons clarifié précédemment, coder avec succès pour ce canal requiert l'application d'une technique de gestion de l'interférence robuste à l'incertitude canal. La construction de techniques de codage alternatives aux techniques actuelles passe la complète compréhension de l'effet du couplage entre incertitude canal et interférence. Nous commençons donc par des exemples qui illustrent de manière intuitive les limitations des techniques existantes face à l'incertitude canal.

Canaux de diffusion à incertitude ordonnés

Un bien simple exemple de canaux ordonnés sur lequel l'incertitude canal a un effet drastique consiste en le canal de diffusion dégradé où les deux récepteurs Y et Z sont ordonnés en terme de capacité de décodage. La stratégie optimale pour de tels canaux (lorsque ceux ci sont bien connus) requiert l'application d'une superposition de deux mots de code. Le mot de code commun, de la couché inférieure, est dédié à l'utilisateur dont le canal est de moindre qualité, disons Y. Le plus fort décodeur Z décode lui les deux mots de codes. La région de débits obtenue est alors de la forme:

$$\begin{cases} R_1 & \leq & I(X;Y|V) \ , \\ R_2 & \leq & I(V;Z) \ . \end{cases} \tag{1}$$

où la variable aléatoire commune V vérifie la chaîne de Markov donnée par $V \multimap X \multimap (Y,Z)$. Ce schéma de codage est extrêmement sensible à l'ordre des utilisateurs et requiert de la source et des deux décodeurs de choisir les schémas de codage et décodage judicieux.

Dans le cas où les canaux sont incertains, la source peut difficilement inférer l'ordre des canaux préalablement au codage et l'application du mauvais schéma de codage résulte en une grande perte au niveau des débits atteignables Fig. 6.

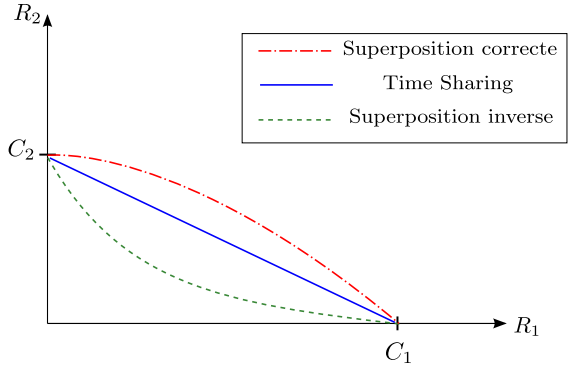


Figure 6: Comparaison des schémas de superposition.

Afin de contrecarrer cette limitation, nous proposons dans le premier chapitre de cette thèse le prince de "Décodage de l'interférence" qui se base sur un codage symétrique l'encodage à la Marton [3], indépendant de l'ordre des canaux, tout en permettant de retrouver le résultat optimal de la superposition de codes. Cela passe par une technique de décodage plus évoluée laissant à chacun des décodeurs le choix de décoder ou non l'interférence. Cette stratégie s'avère judicieuse dans des scénarios où disons deux possibles réalisations d'un utilisateur Y_1 and Y_2 pourrait requérir deux stratégies de codage antagonistes puisque inversement ordonnés par rapport à l'utilisateur opposé Z.

Ceci dit, afin d'identifier des classes de canaux à incertitude pour lesquelles le décodage d'interférence peut s'avérer strictement meilleur que le non-décodage d'interférence, une étude exhaustive de l'effet du couplage de l'interférence et de l'incertitude canal s'impose. Il s'avère que pour la plupart des canaux de diffusion ordonnés pour lesquels la capacité est connue, (canaux à bruit blanc additifs, canaux binaires symétriques, canaux binaires à effacement), le canal à incertitude revient souvent à un canal de diffusion pour la pire

paire de canaux, ceci est dû essentiellement à la relation de dégradation physique ou stochastique entre les canaux respectifs de chaque utilisateur [4].

Cette trivialité est due au fait que la superposition de codes dans l'ordre approprié pour la pire paire de canaux (Y_1, Z) n'affecte pas la meilleure paire de canaux (Y_2, Z). La Fig. 7 illustre cet effet là pour une paire de classe de 2 par 1 canaux de diffusion à incertitude, où Z est dégradé par rapport à Y_1 tandis que Y_2 est dégradé par rapport à Z.

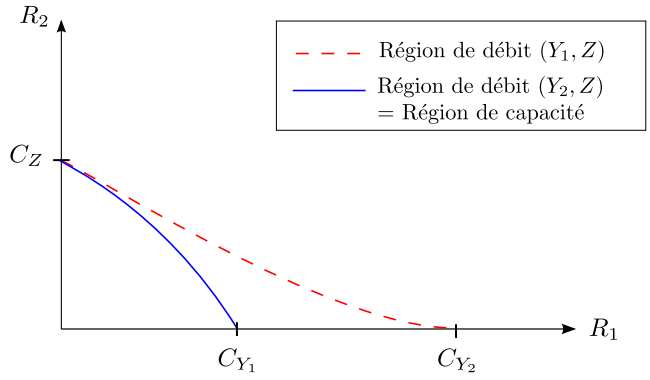


Figure 7: Classe de canaux à incertitude non pertinente

Contribution Au chapitre Premier de cette thèse, nous évaluons le rôle que la stratégie de Décodage d'interférence peut apporter aux classes de canaux de diffusion à incertitude. Après caractérisation de la classe de canaux pour lesquels cette stratégie ne peut être d'une aucune utilité, nous construisons une classe appropriée de 2 par 1 canaux de diffusion à incertitude. Cette classe de canaux nécessite des stratégies de codage antagonistes entre les deux canaux de diffusion. Dans ce cas, le gain qu'apporte le décodage d'interférence est manifeste et a été avéré.

Canaux de diffusion à incertitude non-ordonnés

Lorsque les canaux possibles ne sont pas ordonnés d'une quelconque manière, il devient alors nécessaire de précoder pour l'interférence à la source à travers la technique de "random binning". Une région de débit atteignable lorsque l'interférence V, resp U, est précodée par la source [3] est donnée par $\mathcal{R}_1$, resp. $\mathcal{R}_2$:

$$\mathcal{R}_1 : \begin{cases} R_1 \leq I(U;Y) - I(U;V) , \\ R_2 \leq I(V;Z) , \end{cases} \quad \mathcal{R}_2 : \begin{cases} R_1 \leq I(U;Y) , \\ R_2 \leq I(V;Z) - I(U;V) . \end{cases}$$

où les deux variables aléatoires auxiliaires vérifient la chaîne de Markov $(U, V) \multimap X \multimap (Y, Z)$.

L'une des classes les plus connues pour lesquelles cette stratégie est optimale est le canal de diffusion à antennes multiples "MIMO", et dans ce cas là, la région de capacité est donnée par l'application du principe de "codage sur papier raturé" (Dirty Paper Coding)[16] afin d'annuler l'interférence aux deux utilisateurs [5]. La variable auxiliaire U est alors donnée par $U = X_u + \alpha V$ et $X = X_u + V$ où α est un paramètre qui dépend de la

matrice canal et des niveaux de bruits. A nouveau, lorsque la source ignore quel canal est présent, le choix d'un paramètre α non adapté à la réelle matrice canal est sous-optimal, surtout à fort SNR 8.

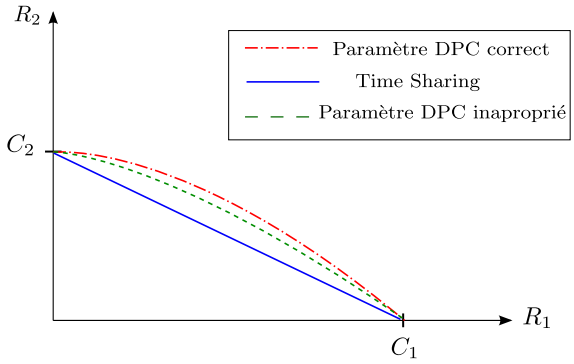


Figure 8: Comparaison de deux schémas DPC pour le canal de diffusion MISO à incertitude

Afin de pallier à cette limitation, nous introduisons au Chapitre Second l'idée de "descriptions multiples" qui consiste à générer, en plus d'une description commune qui doit être décodée aux deux canaux possibles d'un utilisateur, deux descriptions privées décodée chacune à une instance de canal. Ces descriptions privées transmettent différemment l'information pour chacun des deux utilisateurs à travers des constantes de DPC adaptées à ces instances. Elles améliorent donc le débit disponible à chacun des utilisateur, mais résultent en une perte équivalente à leur prix de corrélation.

Dans ce cas aussi, nous remarquons que lorsque l'incertitude canal n'est pas couplée à l'interférence- canal de diffusion standard ou canal point-à-point avec incertitude, le codage à descriptions multiples n'améliore pas les performances du codage avec description commune, i.e codage de Marton. Ceci dit, lorsque interférence et incertitude canal sont couplées, le gain est assez conséquent et nous démontrons cela pour une classe de canaux avec incertitude à antennes multiples.

Contribution Le principal apport de cette thèse est de démontrer que, puisque l'utilisation d'un codage DPC avec uniquement une description commune impose un compromis très fort sur le paramètre DPC utilisé α, alors recourir à des descriptions privées multiples une pour chaque canal ne peut qu'améliorer les performances des schémas de communication. Le point clé de la preuve étant que le coût de corrélation résultant de l'introduction de multiples descriptions est beaucoup moindre que le gain correspondant. Ce gain est davantage manifeste que les canaux incertains sont orthogonaux.

3 Le canal à interférence cognitif avec transmission simultanée

Une deuxième classe de canaux qui apparaissent dans les architectures des réseaux de nouvelle génération est la classe des Canaux à InterFérence Cognitifs ainsi qu'initialement

introduits par Devroye *et.al* [6]. Ce canal modélise un canal à interférences dans lequel une des sources connaît de manière parfaite et non-causale le message de l'autre source. Ce modèle est bien riche en ce qu'il peut modéliser différents scénarios de communication incluant: le canal à interférences avec coopération unilatérale, canal à interférences avec ensemble de messages dégradé, ainsi que la classe des canaux de diffusion avec noeud auxiliaire.

Le CIFC englobe trois scénarios de communication et impose donc que tout schéma de codage combine le schéma optimal pour chacun de ces scénarios: le codage de superposition et "random binning" pour le canal à diffusion formé par $X_2 \to (Y, Z)$, distribution de débits pour le canal à interférences $(X_1, X_2) \to (Y, Z)$ et au final la corrélation des mots de code (X_1, X_2) afin de transmettre le message W_1 sur le canal à accès multiple $(X_1, X_2) \to Y$. Bien que la région de capacité soit encore méconnue pour ce canal, elle a

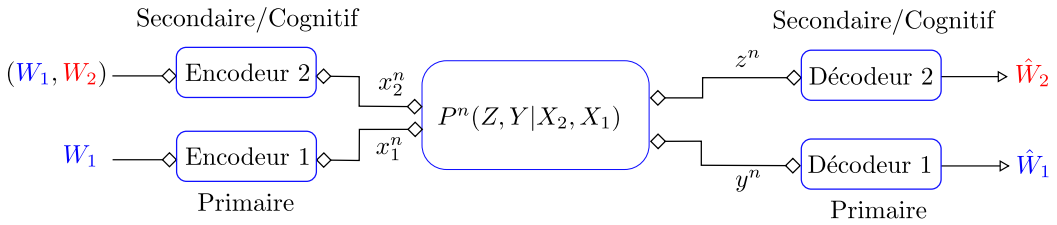


Figure 9: Le Canal à Interférence Cognitif

toutefois été pleinement caractérisée pour différents régimes d'interférences. En présence de très fortes interférences la stratégie optimale est de faire décoder aux deux utilisateurs Y et Z leurs interférences respectives ce qui mène à la région de débits suivante [7]:

$$\begin{cases} R_2 & \leq & I(X_2; Z|X_1) \\ R_1 + R_2 & \leq & I(X_1 X_2; Y) \ . \end{cases} \tag{2}$$

Lorsque les interférences sont très faibles, la stratégie optimale est de faire décoder tous les signaux au décodeur du message cognitif tandis que le décodeur primaire ne décode que son mot de code dédié. La région de capacité qui en résulte est telle [8]:

$$\begin{cases} R_1 & \leq & I(UX_1; Y) \\ R_2 & \leq & I(X_2; Z|UX_1) \ . \end{cases} \tag{3}$$

Ceci dit, ces techniques de gestion de l'interférence dépendent fortement des statistiques des canaux Y et Z, ce qui en présence de plusieurs utilisateurs primaires risque d'impacter fortement le choix des techniques optimales de gestion d'interférences.

En conséquent, dans le troisième chapitre de cette thèse, nous étudions le CIFC avec transmissions simultanées où plusieurs utilisateurs primaires sont intéressés par le message primaire W_1. Notre but est de caractériser la région de capacité sous différents régimes d'interférences: très fortes interférences, très faibles interférences et interférences mixtes.

Contribution Les principaux résultats de ce chapitre est que les stratégies optimales de gestion de l'interférence dans les régimes de très fortes et très faibles interférences

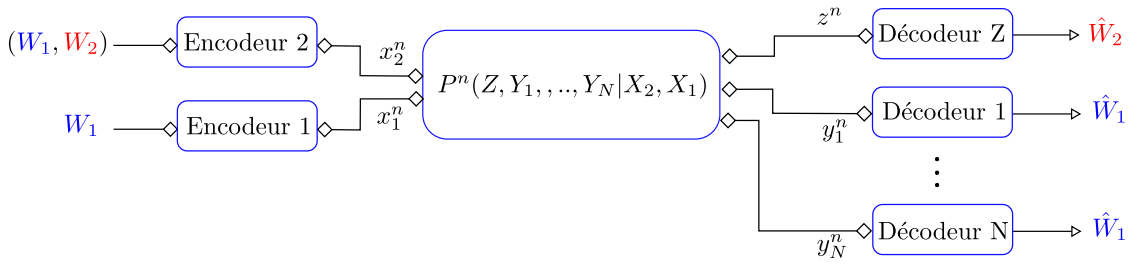


Figure 10: Le Canal à Interférence Cognitif avec transmission multiple

restent optimales même sous transmission multiple. Ceci résulte de l'intuition que si tous les utilisateurs primaires subissent une très forte interférence, ils peuvent la décoder et le décodeur secondaire peut aussi décoder l'interférence qu'il observe. Lorsque tous les utilisateurs primaires subissent de très faibles interférences, la stratégie optimale est que tous considèrent l'interférence comme bruit alors que l'utilisateur secondaire décode l'interférence. Le cas le plus intéressant paraît être le cas mixte où les utilisateurs primaires sont répartis en deux groupes: un groupe subissant de très fortes interférences et un autre subissant de très faibles interférences. La région de capacité de ce cas mixte impose une combinaison très soigneuse des stratégies optimales pour chacun des régimes d'interférences sous-jacents. Nous caractérisons par là même les régions de capacité d'exemples Gaussien en nous basant sur des techniques de construction de mots de codes Gaussiens ainsi que sur des techniques de bornes supérieurs dans le cas Gaussien.

4 Le canal de diffusion avec espion

La sécurité en théorie de l'information a d'abord été introduite par Shannon [9] en étudiant un scénario de communication entre une source, un utilisateur légitime et un utilisateur espion et où la source et l'utilisateur légitime ont accès à une clé de sécurité à travers un lien dédié. Le résultat plutôt pessimiste auquel aboutit Shannon stipule que, afin d'atteindre une sécurité parfaite, le débit de la clé de sécurité doit être au moins aussi élevé que le débit du message à transmettre. Suite à ces résultats, Wyner [2] s'intéresse à ce problème de transmission sécurisée et le formalise par le canal à espion.

Dans un canal à espion, la source et l'utilisateur légitime ne partageant pas de clé de sécurité, la transmission d'un message se doit 'être à la fois sécurisée et fiable. La sécurité est avérée lorsque l'incertitude du noeud espion concernant le message transmis, l'équivoque, $\frac{1}{n}H(W|Z^n)$ est maximale.

Dans le cas d'une sécurité parfaite, la distribution de probabilité du message transmis conditionnelle au signal observé par le noeud espion se doit donc d'être uniforme sur l'ensemble de messages possibles $\lim_{n\to\infty} \frac{1}{n}H(W|Z^n) = R$. L'on dit dans ce cas là qu'il n'y a pas de fuite d'information au noeud espion. Le résultat surprenant de Wyner est que, même sans recourir à une clé de sécurité, l'on peut atteindre une équivoque élevée, voire même une sécurité parfaite.

Ainsi que formalisé, le canal à espion traduit parfaitement le compromis entre la

fiabilité de la transmission, qui requiert des débits assez faibles pour être décodables au noeud légitime, et la sécurité qui elle requiert des débits assez élevés afin de mettre à l'échec la capacité de décodage du neoud espion. La stratégie optimale de codage pour des canaux à espion sans clé de sécurité, rédie dans l'idée du codage stochastique qui consiste à noyer le signal utile dans un bruit de fond afin d'empêcher le noeud espion de distinguer le signal utile du bruit. Ceci dit, le niveau de bruit doit être assez bas pour permettre au noeud légitime de décoder le message qui lui est destiné. La capacité sécurisée est donnée alors par:

$$C_s = \sup_{P_{UX}} [I(U;Y) - I(U;Z)] \tag{4}$$

Ainsi que l'on peut le remarquer, ceci requiert implicitement que l'utilisateur légitime observe une sortie de canal de qualité meilleure que celle du canal du noeud espion, ce qui est en soi une contrainte naturelle vu qu'aucune sécurité de la couche physique ne peut être atteinte dans le cas contraire (à moins de recourir à une clé de sécurité partagée).

Dans la dernière partie de cette thèse, nous étudions le canal de diffusion avec espion Fig. 11, dans lequel une source désire communiquer deux messages à deux utilisateurs tout en les gardant secrets par rapport à un noeud espion externe aux deux utilisateurs légitimes.

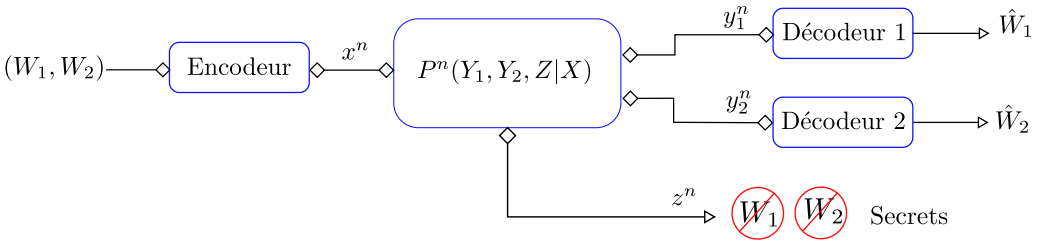


Figure 11: Le canal de diffusion avec espion

Notre but a été d'inférer la meilleure stratégie de gestion des interférences dans pareil scénario en combinant les techniques optimales pour le canal à diffusion et la technique de codage stochastique. L'encodage que l'on applique émane donc de la remarque que, afin de sécuriser les messages simultanément, il ne suffit pas de les sécuriser de manière individuelle; il faut pour ce faire les sécuriser conjointement – ce qui a fortiori mène à des sécurisations individuelles – et la contrainte à satisfaire est la suivante:

$$\lim_{n\to\infty} \frac{1}{n} H(W_1 W_2 | Z^n) = R_1 + R_2. \tag{5}$$

En nous basant donc sur la borne interne de Marton pour le canaux à diffusion, nous utilisons les mots de codes privés afin de sécuriser les messages indépendamment, ceci dit, ils doivent sécuriser de manière conjointe les deux messages. La borne interne qui en résulte s'avère contenir toutes les régions de capacité déjà connues.

Contribution Si les bornes internes à la région de capacité sécurisée ne présentent pas de difficulté majeure dans en dépit des généralisations nécessaires, les bornes externes elles s'avèrent plus fastidieuses. La raison est que les outils existants ne parviennent pas à

écrire des bornes utiles à plus de 2 sorties de canaux. Afin de pallier cette difficulté, nous élaborons une technique de bornes externes en deux étapes. La première étape repose sur une application de l'inégalité de Fano et des contraintes de sécurité afin d'écrire une borne externe en lettre simple pour la région de capacité sécurisée. Ensuite, nous écrivons une formulation équivalente de cette borne externe en montrant qu'une paire de variables auxiliaire n'est pas nécessaire lors de l'optimisation sur l'ensemble des lois de probabilités jointes. En nous basant sur cette borne externe, nous pouvons alors caractériser pleinement la région de capacité sécurisée pour plusieurs classes de canaux de diffusion avec espion jusque lors méconnues.

Chapitre Premier: Canaux de diffusion avec incertitude

1 Introduction

Le canal à diffusion, ainsi que défini par Cover [1] consiste en une source qui souhaite transmettre deux messages privés à deux utilisateurs distincts. Cette classe de canaux a fait l'objet d'importants travaux de recherche afin de caractériser la région de capacité, le principal aspect limitant étant la gestion de l'interférence. Dans cette thèse, nous étudions un canal de diffusion où les deux utilisateurs peuvent avoir un parmi plusieurs canaux possibles, communément désigné par "canal de diffusion avec incertitude". Dans cette classe de canaux, la distribution de probabilité durant la communication est supposée méconnue de la source, mais constante tout au long de la transmission. Afin que la transmission se solde par un succès - probabilité d'erreur au décodeurs nulle- il est nécessaire que la source code pour tous les canaux comme s'ils étaient tous présents simultanément. Notre but est donc de construire des schémas de codage et de décodage afin de s'affranchir de l'interférence couplée à cette incertitude qu'a la source concernant les canaux réellement présents lors de la communication.

Afin de caractériser au mieux les stratégies optimales de gestion de l'interférence avec incertitude canal, nous nous intéressons d'abord aux stratégies optimales en absence d'incertitude: lorsque les canaux des deux utilisateurs sont parfaitement connus de la source. Le meilleur schéma de codage connu à ce jour est celui de Marton [3] qui combine deux stratégies clés du codage pour les réseaux de diffusion: la superposition de codes et le "binning" aléatoire. La superposition de code s'est avérée cruciale dans toutes les classes de canaux de diffusion dont les utilisateurs sont ordonnés de par la qualité de leur canaux: canaux dégradés, moins bruyants, plus capables, essentiellement moins bruyants, essentiellement plus capables [10] ... Le codage reposant sur un principe de "binning" aléatoire est lui par contre optimal pour différentes classes de canaux non-ordonnés: canaux déterministes [11], canaux à antennes multiples [5], canaux produits [12].

Dans cette thèse, nous nous sommes intéressés particulièrement à deux classes de canaux: canaux à incertitudes ordonnés et canaux à incertitude à antennes multiples (non-ordonnés). Pour la première classe de canaux, nous élaborons un nouveau schéma de "Décodage" basé sur une technique de "Décodage de l'interférence" qui consiste à laisser à chaque utilisateur le choix de décoder ou non l'interférence de l'utilisateur opposé. Lors de l'application d'un tel principe, nous remarquons que la région de débit résultante contient différents schémas de transmission correspondants aux différents ordres de superposition

de codes. Par conséquent, il apparaît que la source peut appliquer un schéma de codage totalement symétrique et que les décodeurs, en choisissant la bonne stratégie de décodage, peuvent recréer les régions dé débit de la superposition de code optimale. Notre but a donc été de démontrer que pour une certaine classe de canaux, cette stratégie était nécessaire et qu'en l'absence de son application – en appliquant un schéma de codage de Marton naif – il était impossible d'atteindre les mêmes performances.

Or, lorsque les canaux ne sont pas ordonnés, à l'exemple des canaux à antennes multiples, la stratégie optimale n'est donc plus de décoder l'interférence, mais plutôt de la précoder à la source. Ce précodage – à travers le schéma de codage sur papier raturé (Dirty Paper Coding) – nécessite la connaissance parfaite des canaux à la source. Lorsque cette connaissance est défaillante, les débits atteints s'en trouvent fortement diminués, voire même moins importants qu'une simple division en temps des deux transmissions. Dès lors, il devient important de trouver des schémas de codage (à la source) qui permettent de pallier cette méconnaissance du canal, ce que l'on suggère à travers l'introduction de descriptions multiples. A chaque instance de canal d'un utilisateur est dédiée une description privée précodant le signal dans une direction privilégiée pour cet utilisateur, en plus d'une description commune à toutes ces instances. L'on montre à travers un exemple Gaussien l'importance et le gain d'une telle stratégie contrairement à une approche où l'on ne transmettrait qu'une description commune à toutes les instances de canaux possibles.

Dans ce qui suit sont listés les principaux résultats de ces deux approches de codage et décodage permettant de pallier à l'incertitude du canal à la source et dont on pourra ultérieurement discuter une possible combinaison.

2 Décodage de l'interférence

La borne inférieure que nous énonçons par la suite rejoint le raisonnement dans [13]. Le principe de "décodage de l'interférence", introduit dans [14], permet à chaque décodeur de décoder ou non l'interférence de l'autre utilisateur.

Theorem 1 (Borne interne de Décodage de l'Interférence)**.** *Une borne interne à la région de capacité du canal à diffusion est définie par l'ensemble des triplets de débits* (R_0, R_1, R_2) *inclus dans:*

$$\mathcal{R}_{ID} \triangleq \bigcup_{p_{QUVX}\in\mathcal{P}} \underbrace{\bigcup_{(T_1,T_2)\in\mathbb{T}(p)}}_{FME} \underbrace{\bigcap_{j=1}^{N\times M}}_{(compound)} \underbrace{\bigcup_{i_j=1}^{4}}_{(4\ methods)} \mathcal{T}_{i_j}^{(j)}(p,T_1,T_2)\ , \tag{1}$$

où $\mathcal{P}$ *est l'ensemble des distributions de probabilités jointes* p_{QUVX} *vérifiant* $(Q,U,V) \multimap X \multimap (Y_1,\ldots,Y_N,Z_1,\ldots,Z_N)$.
Les régions de débit $\mathcal{T}_{[1:4]}^{(j)}$ *et l'ensemble* $\mathbb{T}$ *sont, eux, définis respectivement par:*

$$\mathcal{T}_1^{(j)}(p,T_1,T_2): \begin{cases} T_1 \leq I(U;Y_j|Q)\ , \\ R_0+T_1 \leq I(QU;Y_j)\ , \\ T_2 \leq I(V;Z_j|Q)\ , \\ R_0+T_2 \leq I(QV;Z_j)\ , \end{cases} \tag{2}$$

$$\mathcal{T}_2^{(j)}(p,T_1,T_2):\begin{cases} T_1 \leq I(U;Y_j|Q)\ , \\ R_0+T_1 \leq I(QU;Y_j)\ , \\ T_2 \leq I(V;Z_jU|Q)\ , \\ T_1+T_2 \leq I(UV;Z_j|Q)+I(U;V|Q)\ , \\ R_0+T_1+T_2 \leq I(QUV;Z_j)+I(U;V|Q)\ , \end{cases} \tag{3}$$

$$\mathcal{T}_3^{(j)}(p,T_1,T_2):\begin{cases} T_1 \leq I(U;Y_jV|Q)\ , \\ T_1+T_2 \leq I(UV;Y_j|Q)+I(U;V|Q)\ , \\ R_0+T_1+T_2 \leq I(QUV;Y_j)+I(U;V|Q)\ , \\ T_2 \leq I(V;Z_j|Q)\ , \\ R_0+T_2 \leq I(QV;Z_j)\ , \end{cases} \tag{4}$$

$$\mathcal{T}_4^{(j)}(p,T_1,T_2):\begin{cases} T_1 \leq I(U;Y_jV|Q)\ , \\ T_1+T_2 \leq I(UV;Y_j|Q)+I(U;V|Q)\ , \\ R_0+T_1+T_2 \leq I(QUV;Y_j)+I(U;V|Q)\ , \\ T_2 \leq I(V;Z_jU|Q)\ , \\ T_1+T_2 \leq I(UV;Z_j|Q)+I(U;V|Q)\ , \\ R_0+T_1+T_2 \leq I(QUV;Z_j)+I(U;V|Q)\ , \end{cases} \tag{5}$$

$$\mathbb{T}(p)=\Big\{(T_1,T_2):\quad T_1 \geq R_1\ , \tag{6}$$

$$T_2 \geq R_2\ , \tag{7}$$

$$T_1+T_2 > R_1+R_2+I(U;V|Q)\Big\}\ . \tag{8}$$

Afin d'aboutir à cette région de capacité, chaque utilisateur instancie deux listes, ce qui résulte in fine en l'union de quatre région, où:

1. La région $\mathcal{T}_1^{(j)}$ n'est autre que la région de Marton,
2. La région $\mathcal{T}_4^{(j)}$ est obtenue en faisant décoder aux deux utilisateurs les deux signaux,
3. Les régions $\mathcal{T}_2^{(j)}$ et $\mathcal{T}_3^{(j)}$ correspondent au cas où un utilisateur parmi les deux décode l'interférence alors que l'autre la considère comme bruit.

L'on peut alors observer que dans le cas d'incertitude du canal, l'on obtient une région de débit apparemment plus grande que celle obtenue par le codage simple à la Marton, en ce que

$$\mathcal{R}_{\text{NID}} \triangleq \bigcup_{p_{QUVX}\in\mathcal{P}} \bigcup_{(T_1,T_2)\in\mathbb{T}(p)} \left(\bigcap_{j=1}^{N\times M} \mathcal{T}_1^{(j)}(p,T_1,T_2) \right)\ . \tag{9}$$

Ceci dit, cette inclusion peut s'avérer non-stricte (comme on peut le démontrer en l'absence d'incertitude).

Par la suite, nous identifions une classe de canaux de diffusion avec incertitude du canal pour laquelle cette inclusion est stricte en montrant que la région obtenue par le décodage d'interférence atteint la capacité du canal, alors que le codage à la Marton reste strictement sous optimal.

Afin d'étudier une classe intéressante de canaux, supposons que l'on est dans un modèle où:

Table 1: Différents ordres permis par le canal à diffusion BEC(e)/BSC(p).

$0 \leq e \leq 2p$	$2p < e \leq 4p(1-p)$	$4p(1-p) < e \leq H_2(p)$	$H_2(p) < e \leq 1$
BSC degradé de BEC	BEC Moins Bruyant BSC	BEC Plus Capable BSC	BSC Ess. Moins bruyant BEC

- L'utilisateur 2 n'a pas d'incertitude sur son canal, i.e., $Z_1 = Z_2 = Z$.
- L'utilisateur 1 peut observer un des deux canaux $\{Y_j\}_{j\in\{1,2\}}$.

Afin de montrer la stricte inclusion $\mathcal{R}_{\text{NID}} \subset \mathcal{R}_{\text{ID}}$, la classe de canaux retenue doit être non-triviale, i.e, (Y_1, Y_2) ne doivent pas être fortement ordonnés car sinon, il suffit de coder pour le pire canal; il est nécessaire par ailleurs que les canaux de diffusion formés par les deux paires possibles (Y_1, Z) et (Y_2, Z) soient ordonnés dans deux sens différents.

Les canaux retenus sont les canaux de diffusion formés par un canal binaire symétrique et un canal binaire à effacement, qui présentent l'avantage de permettre plusieurs nuances d'ordre selon le choix des probabilités de transition p et d'effacement e ainsi que donnés dans le Tableau 1.

Nous définissons alors le canal à diffusion avec incertitude suivant:

$$\mathcal{W} : \begin{cases} \mathcal{X} & \longmapsto & \mathcal{Z} \equiv \text{BSC(p)}\,, \\ \mathcal{X} & \longmapsto & \mathcal{Y}_1 \equiv \text{BSC}(p_1)\,, \\ \mathcal{X} & \longmapsto & \mathcal{Y}_2 \equiv \text{BEC}(e_2)\,. \end{cases} \tag{10}$$

En choisissant les paramètres du modèle tels que:

$$4p(1-p) < 4p_1(1-p_1) < e_2 \leq H_2(p) \leq H_2(p_1)\ , \tag{11}$$

nous assurons que les deux critères d'intérêt du modèle sont satisfaits: absence d'ordre fort, et ordres antagonistes sur les deux canaux de diffusion possibles.

Dans ce cas là, nous pouvons montrer qu'une borne supérieure possible pour ce canal à incertitude consiste en:

$$\mathcal{C}_1 : \begin{cases} R_1 & \leq & 1 - H_2(p_1 \star \alpha)\ , \\ R_2 & \leq & H_2(p \star \alpha) - H_2(p)\ , \end{cases} \tag{12}$$

où $\alpha \in [0 : 0.5]$, H_2 est l'entropie binaire et $\star$ est l'opérateur de convolution binaire.

2.1 Le décodage de l'interférence atteint la région de capacité

Nous évaluons la région de décodage d'interférence en faisant décoder à (Y_2, Z) leur interférences, et en imposant à Y_1 (le pire de tous les utilisateurs) de ne décoder que son signal utile. La région de débit résultante est telle que:

$$\begin{cases} R_1 & \leq & I(\bar{Q}; Y_1)\ , \\ R_1 + R_2 & \leq & I(\bar{Q}; Y_1) + I(X; Z|\bar{Q})\ . \end{cases} \tag{13}$$

où $\bar{Q} = QU$. En évaluant cette région avec un choix binaire où: $\bar{Q} \longmapsto X \equiv \text{BSC}(\alpha)$ et $X \sim \text{Bern}(1/2)$, nous obtenons l'union sur tout $\alpha \in [0 : .5]$ de la région de débit:

$$\mathcal{R}_{\text{ID}} : \begin{cases} R_1 & \leq & 1 - H_2(p_1 \star \alpha)\ , \\ R_1 + R_2 & \leq & 1 - H_2(p_1 \star \alpha) + H_2(p \star \alpha) - H_2(p)\ . \end{cases} \tag{14}$$

qui n'est autre que la région de capacité.

Pour ce qui est de la région de codage à la Marton, nous pouvons montrer qu'elle est incluse dans la région de débit définie par:

$$\mathcal{R}_{\text{OuterNID}} : \begin{cases} R_1 & \leq & \min\limits_{j=1,2} I(\bar{Q};Y_j) \ , \\ R_1+R_2 & \leq & I(X;Z|\bar{Q}) + \min\limits_{j=1,2} I(\bar{Q};Y_j) \ . \end{cases} \tag{15}$$

Afin d'évaluer cette région, nous montrons qu'il suffit de choisir des variables telles que $\|\bar{Q}\| \leq 4$ et $X \sim \text{Bern}(1/2)$. Ceci dit, la distribution qui maximise cette région est relativement complexe à caractériser. Pour ce, nous choisissons de borner analytiquement les débits engendrés par cette région, $\mathcal{R}_{\text{Outer,NID}}$, à travers la fonction trajectoire qui la définit: $t : [0 : 1 - H_2(p)] \mapsto \Re_+$ telle que

$$t(x) \triangleq \sup_{p_{XQ} \in \mathcal{C}(x)} \min\{I(Q;Y_1), I(Q;Y_2)\} \tag{16}$$

$$= \sup_{p_{XQ} \in \mathcal{C}(x)} \min_{a \in [0:1]} [aI(Q;Y_1) + (1-a)I(Q;Y_2)] \tag{17}$$

et où la classe $\mathcal{C}(x)$ est donnée par:

$$\mathcal{C}(x) = \Big\{ p_{XQ} \in \mathcal{P}(\mathcal{X} \times \mathcal{Q}) : \quad Q \multimap X \multimap (Z, Y_1, Y_2) \\ X \sim \text{Bern}(1/2) \ , \ I(X;Z|Q) \geq x \Big\} \ . \tag{18}$$

De la même manière, si l'on définit t_1

$$t_1(x) \triangleq \sup_{p_{XQ} \in \mathcal{C}(x)} I(Q;Y_1) \ , \tag{19}$$

alors t_1 caractérise pleinement la région de capacité $\mathcal{C}_1$.

Le principal résultat que nous démontrons est qu'une borne supérieur de la région de débit à la Marton est donnée par:

$$t_a(x) = \inf_{\lambda \in \mathcal{R}^+} \left[\max_{\mathcal{P}(\mathcal{X} \times \mathcal{Q})} \Big[a\, I(Q;Y_1) + \bar{a}\, I(Q;Y_2) + \lambda\, I(X;Z|Q) \Big] - \lambda\, x \right] \tag{20}$$

$$= \inf_{\lambda \in \mathcal{R}^+} \Big[F_a(\lambda) - \lambda\, x \Big] \ , \tag{21}$$

where

$$F_a(\lambda) \triangleq \max_{p_{XQ} \in \mathcal{P}(\mathcal{X} \times \mathcal{Q})} \Big[a\, I(Q;Y_1) + \bar{a}\, I(Q;Y_2) \Big] \ . \tag{22}$$

et est strictement inférieur à t_1 dans un intervalle de points.

Dans la Fig. 1, nous choisissons $a = 0.92$ et traçons la fonction de différence normalisée:

$$d_a(R_1) = \frac{t_1^{-1}(R_1) - t_a^{-1}(R_1)}{\max(\mid t_1^{-1}(R_1) - t_a^{-1}(R_1) \mid)} \ , \tag{23}$$

sur l'intervalle pertinent: $[0 : 1 - H_2(p_1 \star \alpha_0)]$ où $1 - H_2(p_1 \star \alpha_0) = (1 - e_2)(1 - H_2(\alpha_0))$. La fonction d_a étant strictement positive, l'inclusion stricte est démontrée.

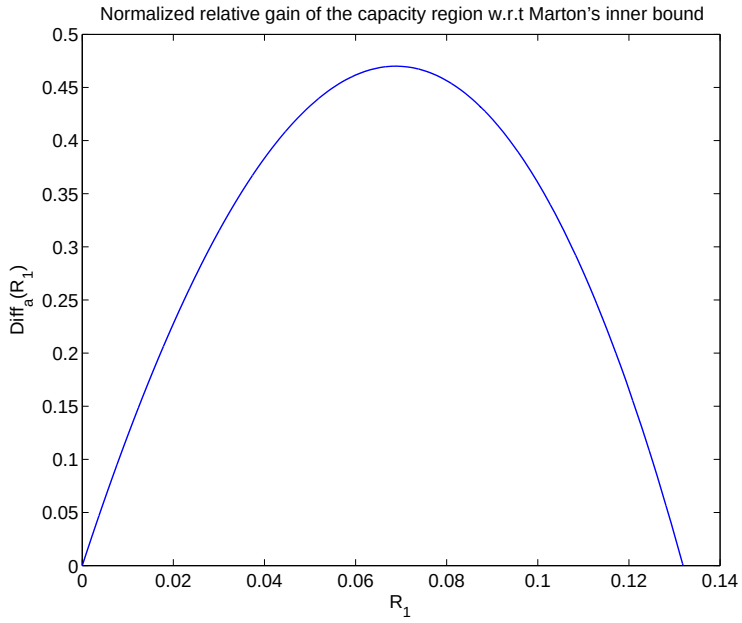


Figure 1: $d_a(R_1)$ fonction de différence normalisée pour $a = 0.92$, $e_2 = 0.46$, $p = 0.1$ et $p_1 = 0.13$.

3 Codage à descriptions multiples

Dans cette partie du travail, nous explorons un schéma d'encodage pouvant substantiellement améliorer les performances dans un scénario avec incertitude: Le codage à descriptions multiples.

L'utilité de ce schéma de codage s'avère payante lorsqu'aucune forme d'ordre n'existe entre les canaux du même utilisateur. L'idée principale sur laquelle se base cette méthode de codage consiste à générer pour un groupes de canaux possibles, une description commune que tous seront amenés à décoder, et autant de descriptions privées qui chacune est destinée à une instance de canal possible. La description commune souffre de l'incertitude du canal contrairement aux descriptions privées. Ceci dit, les descriptions privées introduisent un coût de corrélation. Pareil compromis fera donc l'objet de l'étude que nous menons par la suite.

Nous nous intéressons comme précédemment à la classe de canaux la plus simple où seulement un utilisateur parmi les deux est affecté par l'incertitude entre deux canaux possibles: Y_1 or Y_2. Nous écrivons d'abord une borne interne à la région de capacité inspirée par le codage à descriptions multiples et nous comparons pour une classe de canaux à antennes multiples (MISO), ce schéma de codage au schéma où l'on n'a recourt qu'à une seule description.

Theorem 2 (MD inner bound)**.** *La région de capacité du canal à incertitude étudié contient toutes les paires de débits* (R_1, R_2) *vérifiant:*

$$R_1 \leq I(U_0U_1; Y_1|Q) \ , \tag{24a}$$

$$R_1 \leq I(U_0U_2;Y_2|Q)\ , \tag{24b}$$
$$2R_1 \leq I(U_0U_1;Y_1|Q) + I(U_0U_2;Y_2|Q) - I(U_1;U_2|QU_0)\ , \tag{24c}$$
$$R_2 \leq I(V;Z|Q)\ , \tag{24d}$$
$$R_1 + R_2 \leq I(U_0U_1;Y_1|Q) + I(V;Z|Q) - I(U_0U_1;V|Q)\ , \tag{24e}$$
$$R_1 + R_2 \leq I(U_0U_1;Y_2|Q) + I(V;Z|Q) - I(U_0U_2;V|Q)\ , \tag{24f}$$
$$\begin{aligned} 2R_1 + R_2 \leq\ & I(U_0U_1;Y_1|Q) + I(U_0U_2;Y_2|Q) + I(V;Z|Q) \\ & - I(U_0U_1U_2;V|Q) - I(U_1;U_2|QU_0)\ , \end{aligned} \tag{24g}$$
$$\begin{aligned} 2R_1 + 2\,R_2 \leq\ & I(U_0U_1;Y_1|Q) + I(U_0U_2;Y_2|Q) + 2I(V;Z|Q) \\ & - I(U_0U_1;V|Q) - I(U_0U_2;V|Q) - I(U_1;U_2|QU_0V)\ , \end{aligned} \tag{24h}$$

pour une distribution de probabilité jointe $P_{QU_0U_1U_2VX}$ satisfaisant la chaîne de Markov suivante: $(Q,U_0,U_1,U_2,V) \multimap X \multimap (Y_1,Y_2,Z)$.

En contrepartie, lorsque nous ne recourrons qu'à une description commune (codage à la Marton) nous pouvons écrire ce que nous dénommons par la suite la région de débits à description commune (CD) qui consiste en toutes les paires de débits (R_1,R_2) vérifiant:

$$R_1 \leq \min_{j\in\{1,2\}} I(U;Y_j|Q)\ , \tag{25a}$$
$$R_2 \leq I(V;Z|Q)\ , \tag{25b}$$
$$R_1 + R_2 \leq \min_{j\in\{1,2\}} I(U;Y_j|Q) + I(V;Z|Q) - I(U;V|Q)\ , \tag{25c}$$

où U, V et Q sont des variables auxiliaires arbitrairement corrélées. Nous pouvons dores et déjà remarquer qu'en supposant $U_1 \equiv \emptyset$ et $U_2 \equiv \emptyset$, la région aux descriptions multiples contient alors la région à description commune. Notre but est donc montrer que cette inclusion est stricte pour une classe de canaux donnés: les canaux à antennes multiples.

3.1 Le canal à antennes multiples (MISO) avec incertitude

La stratégie de transmission optimale pour la classe de canaux de diffusion à antennes multiples est l'application d'un codage sur papier raturé (Dirty Paper Coding) ainsi que suggéré dans [15, 16]. Nous adaptons donc cette stratégie avec l'introduction de descriptions privées à la classe de canaux avec incertitude en construisant un MD-DPC que nous comparons par la suite au schéma n'invoquant qu'un seule description commune que nous dénotons CD-DPC.

Le modèle de canal retenu est le suivant:

$$\left\{ \begin{array}{rcl} y_{j,i} & = & \mathbf{h}_j^t\,\mathbf{x}_i + n_{j,i}\ , \\ z_i & = & \mathbf{g}^t\,\mathbf{x}_i + w_i\ , \end{array} \right. \tag{26}$$

où $j \in \{1,2\}$,et où $\mathbf{h}_j$ et $\mathbf{g}$ sont des vecteurs réels de taille 2×1 linéairement indépendants deux à deux. $\mathbf{x}$ est le signal d'entrée du canal 2×1 et vérifie la contrainte de puissance $\mathbb{E}[\mathbf{x}^t\mathbf{x}] \leq P$ alors que les séquences de bruits $\{n_{j,i}\}$ et $\{w_i\}$sont supposées i.i.d. suivant une loi normale de puissance N: $\mathcal{N}(0,N)$.

Dans ce qui suit, nous comparons les performances du schéma de CD-DPC avec celui incluant des descriptions multiples, MD-DPC, mais sous différentes configurations des descriptions privées. Dans un premier cas, nous supposons que chacune des descriptions n'est utilisée qu'une partie du temps de la transmission pour ainsi dire annuler le coût de corrélation en résultant. Ensuite, nous nous intéressons au cas où ces deux descriptions sont complètement corrélées (égales) conditionnellement à la description commune et à l'interférence. Les trois régions de débit résultantes sont données ci-après:

3.2 DPC avec description commune(CD-DPC)

Définissons les deux régions de débit suivantes:

$$\mathcal{R}_1 : \begin{cases} R_1 & \leq & \max\limits_{\alpha} \min\limits_{j\in\{1,2\}} \dfrac{1}{2}\log_2\left(\dfrac{h_{j,u}^2 P_u + N}{I_j(\alpha-\beta_j)^2 + N}\right) , \\ R_2 & \leq & \dfrac{1}{2}\log_2\left(\dfrac{g_u^2 P_u + g_v^2 P_v + N}{g_u^2 P_u + N}\right) , \end{cases} \tag{27}$$

où β_j et I_j sont donnés par:

$$\beta_j = \frac{P_u\, h_{j,u}\, h_{j,v}}{h_{j,u}^2\, P_u + N} \quad \text{and} \quad I_j = \left(\frac{P_v}{P_u}\right) \frac{\left(h_{j,u}^2 P_u + N\right)^2}{h_{j,u}^2 P_u + h_{j,v}^2 P_v + N} \,. \tag{28}$$

La seconde région de débit consiste en les paires de débits vérifiant:

$$\mathcal{R}_2 : \begin{cases} R_2 & \leq & \dfrac{1}{2}\log_2\left(\dfrac{g_v^2 P_v + N}{N}\right) , \\ R_1 & \leq & \min\limits_{j=1,2} \dfrac{1}{2}\log_2\left(\dfrac{h_{j,u}^2 P_u + h_{j,v}^2 P_v + N}{h_{j,v}^2 P_v + N}\right) . \end{cases} \tag{29}$$

Proposition 1 (Région interne à description commune)**.** *Le recours à uniquement une description commune mène à la région de débit suivante:*

$$\mathcal{R}_{\textit{CD-MISO BC}} = \bigcup_{\substack{(P_u,P_v) \\ P_u+P_v\leq P}} \bigcup_{\substack{\mathbf{B}_u,\mathbf{B}_v \\ \|\mathbf{B}_u\|=1 \\ \|\mathbf{B}_v\|=1}} \left[\mathcal{R}_1(\mathbf{B}_u,\mathbf{B}_v,P_u,P_v) \cup \mathcal{R}_2(\mathbf{B}_u,\mathbf{B}_v,P_u,P_v)\right] \,. \tag{30}$$

Ci -après, nous détaillons les deux méthodes de codage à descriptions multiples: décoréllées dans le temps puis totalement corrélées.

3.3 MD-DPC avec descriptions décorrélées

La région à descriptions multiples que nous générons ci-bas est basée sur un argument de multiplexage dans le temps des deux descriptions privées. La description commune ainsi que chacune des descriptions privées appliquent un DPC distinct et la région que nous évaluons est telle:

$$\begin{cases} R_1 & \leq & \min\limits_{j\in\{1,2\}} \Big[I(U_0U_j;Y_j|Q) - I(U_0U_j;V|Q)\Big] \\ 2R_1 & \leq & \sum\limits_{j\in\{1,2\}} \Big[I(U_0U_j;Y_j|Q) - I(U_0U_j;V|Q)\Big] - I(U_1;U_2|U_0VQ) \\ R_2 & = & I(V;Z|Q) \,. \end{cases} \tag{31}$$

Soit Q une variable binaire Bernouilli indexant le multiplexage dans le temps:

$$\mathbb{P}(Q=1) = 1 - \mathbb{P}(Q=2) \triangleq t \ . \tag{32}$$

Dénotons par $\mathcal{R}_u$ la région ci-après:

$$\mathcal{R}_u : \left\{ \begin{array}{rcl} R_1 & \leq & \max\limits_{\alpha} \min\limits_{j\in\{1,2\}} \left\{ \frac{1}{2}\, p_Q(j)\, \log_2 \left(\frac{h_{j,u}^2\, x + N}{N} \right) \right. \\ & & \left. \qquad + \frac{1}{2} \log_2 \left(\frac{h_{j,u}^2 P_u + N}{I_j^x \left(\alpha - \beta_j^x\right)^2 + N + h_{j,u}^2 x} \right) \right\} , \\ R_2 & \leq & \frac{1}{2} \log_2 \left(\frac{g_u^2\, P_u + g_v^2\, P_v + N}{g_u^2\, P_u + N} \right) \ , \end{array} \right.$$

où β_j^x et I_j^x sont choisis tels que:

$$\beta_j^x = \frac{(P_u - x)\, h_{j,u}\, h_{j,v}}{h_{j,u}^2 P_u + N} \quad \text{and} \quad I_j^x = \left(\frac{P_v}{P_u - x} \right) \frac{\left(h_{j,u}^2 P_u + N \right)^2}{h_{j,u}^2 P_u + h_{j,v}^2 P_v + N} \ . \tag{33}$$

Proposition 2 (MD-DPC avec descriptions décorrelées)**.** *Une borne interne de la région de capacité du canal étudié consiste en:*

$$\mathcal{R}_{\textit{MDindep-MISO BC}} = \bigcup_{t\in[0:1]} \bigcup_{\substack{(P_u,,P_v) \\ P_u+P_v\leq P \\ 0\leq x\leq P_u}} \bigcup_{\substack{\mathbf{B}_u,\mathbf{B}_v \\ \|\mathbf{B}_u\|=1 \\ \|\mathbf{B}_v\|=1}} \mathcal{R}_u(\mathbf{B}_u, \mathbf{B}_v, x, t, P_u, P_v) \ . \tag{34}$$

3.4 MD-DPC avec descriptions corrélées

Dans cette partie, nous permettons aux descriptions privées une corrélation dans le temps, voire même une égalité conditionnellement à l'interférence et à la description commune. Définissons donc:

$$\mathcal{R}_c : \left\{ \begin{array}{rcl} R_1 & \leq & \min\{f_1(\alpha, x), f_2(\alpha, x)\} \ , \\ R_1 & \leq & \frac{1}{2} \left[f_1(\alpha, x) + f_2(\alpha, x) - \frac{1}{2} \log_2(2\pi e x) \right] \ , \\ R_2 & \leq & \frac{1}{2} \log_2 \left(\frac{g_u^2 P_u + g_v^2 P_v + N}{g_u^2 P_u + N} \right) \ , \end{array} \right.$$

où:

$$f_j(\alpha, x) \triangleq \frac{1}{2} \log_2 \left(\frac{h_{j,u}^2\, P_u + N}{\frac{I_j^x N (\alpha - \beta_j^x)^2}{h_{j,u}^2 x + N} + N} \right) \ , \tag{35}$$

et β_j^x et I_j^x sont définis par:

$$\beta_j^x = \frac{(P_u - x)\, h_{j,u}\, h_{j,v}}{h_{j,u}^2 P_u + N} \quad \text{and} \quad I_j^x = \left(\frac{P_v}{P_u - x} \right) \frac{\left(h_{j,u}^2 P_u + N \right)^2}{h_{j,u}^2 P_u + h_{j,v}^2 P_v + N} \, . \tag{36}$$

Proposition 3 (MD-DPC avec descriptions corrélées)**.** *Une borne interne à la région de capacité du canal étudié est telle:*

$$\mathcal{R}_{MDcorr\text{-}MISO\ BC} = \bigcup_{\substack{\mathbf{B}_u,\mathbf{B}_v \\ \|\mathbf{B}_u\|=1 \\ \|\mathbf{B}_v\|=1}} \bigcup_{\substack{(P_u,P_v) \\ P_u+P_v\leq P \\ 0\leq x\leq P_u}} \bigcup_{\alpha\in\mathbb{R}} \mathcal{R}_c(\mathbf{B}_u,\mathbf{B}_v,\alpha,x,P_u,P_v)\ . \tag{37}$$

Afin de comparer au mieux les performances de ces trois bornes internes, il serait propice d'évaluer leurs performances par rapport à la meilleure borne externe à la région de capacité que l'on peut écrire pour ce genre de canaux.

3.5 Borne externe à la région de capacité

Pour ce faire, introduisons les canaux augmentés suivants:

$$\mathbf{g}_{1,2} \triangleq [\mathbf{g}\ \mathbf{h}_1\ \mathbf{h}_2]\ , \tag{38}$$
$$\mathbf{h}_{1,z} \triangleq [\mathbf{h}_1\ \mathbf{g}]\ , \tag{39}$$
$$\mathbf{h}_{2,z} \triangleq [\mathbf{h}_2\ \mathbf{g}]\ . \tag{40}$$

Nous notons donc le canal ayant pour marginale celle de la concaténation à la suite des deux canaux $[Z\ Y_1\ Y_2]$ comme étant $Z_{1,2}$, et définissions par là même les deux autres instances de canaux augmentés $Y_{1,z}$ and $Y_{2,z}$.

Theorem 3 (Borne externe à la région de capacité)**.** *La région de capacité du canal étudié est incluse dans l'ensemble des paires de débits:*

$$\mathcal{O} = \mathcal{C}_1 \cap \mathcal{C}_2 \cap \mathcal{C}_{1,2} \cap \mathcal{C}_z\ , \tag{41}$$

où $\mathcal{C}_j$ est la région de capacité du canal de diffusion (Y_j, Z), for $j \in \{1,2\}$,

$$\mathcal{C}_j = \bigcup_{\substack{(\mathbf{K}_u,\mathbf{K}_v) \\ tr(\mathbf{K}_u+\mathbf{K}_v)\leq P}} \Bigg\{ (R_1,R_2)\in\mathbb{R}_+^2\,,$$
$$R_1 \leq \frac{1}{2}\log_2\left(\frac{\mathbf{h}_j^t\mathbf{K}_u\mathbf{h}_j+N}{N}\right) \tag{42}$$
$$R_2 \leq \frac{1}{2}\log_2\left(\frac{\mathbf{g}^t(\mathbf{K}_u+\mathbf{K}_v)\mathbf{g}+N}{\mathbf{g}^t\mathbf{K}_u\mathbf{g}+N}\right) \tag{43}$$
$$or$$
$$R_1 \leq \frac{1}{2}\log_2\left(\frac{\mathbf{h}_j^t(\mathbf{K}_u+\mathbf{K}_v)\mathbf{h}_j+N}{\mathbf{h}_j^t\mathbf{K}_v\mathbf{h}_j+N}\right) \tag{44}$$
$$R_2 \leq \frac{1}{2}\log_2\left(\frac{\mathbf{g}^t\mathbf{K}_v\mathbf{g}+N}{N}\right)\Bigg\}\ , \tag{45}$$

$\mathcal{C}_{1,2}$ est la région de capacité du canal avec incertitude $(Y_1, Z_{1,2})$ / $(Y_2, Z_{1,2})$,

$$\mathcal{C}_{1,2} = \bigcup_{\substack{(\mathbf{K}_u,\mathbf{K}_v) \\ tr(\mathbf{K}_u+\mathbf{K}_v)\leq P}} \Bigg\{ (R_1,R_2)\in\mathbb{R}_+^2\,,$$

$$R_1 \leq \min_{j\in\{1,2\}} \frac{1}{2}\log_2\left(\frac{\mathbf{h}_j^t(\mathbf{K}_u+\mathbf{K}_v)\mathbf{h}_j+N}{\mathbf{h}_j^t\mathbf{K}_v\mathbf{h}_j+N}\right), \tag{46}$$

$$R_2 \leq \frac{1}{2}\log_2\left(\frac{\left|\mathbf{g}_{1,2}^t\mathbf{K}_v\mathbf{g}_{1,2}+N\mathbf{I}_3\right|}{N^3}\right)\Bigg\} \tag{47}$$

et finalement $\mathcal{C}_z$ est la région de capacité du canal à incertitude $(Y_{1,z}, Z)$ / $(Y_{2,z}, Z)$,

$$\mathcal{C}_z = \bigcup_{\substack{(\mathbf{K}_u,\mathbf{K}_v)\\ tr(\mathbf{K}_u+\mathbf{K}_v)\leq P}} \Bigg\{(R_1,R_2)\in\mathbb{R}_+^2\,,$$

$$R_1 \leq \min_{j\in\{1,2\}} \frac{1}{2}\log_2\left(\frac{\left|\mathbf{h}_{j,z}^t\mathbf{K}_u\mathbf{h}_{j,z}+N\mathbf{I}_2\right|}{N^2}\right) \tag{48}$$

$$R_2 \leq \frac{1}{2}\log_2\left(\frac{\mathbf{g}^t(\mathbf{K}_u+\mathbf{K}_v)\mathbf{g}+N}{\mathbf{g}^t\mathbf{K}_u\mathbf{g}+N}\right)\Bigg\}\,. \tag{49}$$

3.6 Conclusions

Nous traçons dès lors les différentes bornes internes et externes relatives à la classe de canaux de diffusion avec incertitude et antennes multiples, et remarquons l'inclusion stricte de la région avec description commune par rapport à la région aux descriptions multiples, ce que l'on confirme aussi de manière plus détaillées analytiquement.

4 Conclusion

Dans ce premier chapitre de thèse, nous explorons de nouvelles techniques d'encodage et de décodage pour les canaux de diffusion avec incertitude. Lorsque les canaux sont ordonnées, nous proposons de recourir au principe de Décodage d'Interférence qui permet de contrecarrer la difficulté d'imposer un ordre d'encodage et de décodage dans connaissance à priori de l'ordre des canaux. Dans le cas où les canaux ne sont pas ordonnés, nous élaborons une technique d'encodage plus apte à transporter l'information de manière optimale pour chacune des instances possibles du canal et copiant le principe de descriptions multiples en codage source. Pour les deux techniques ainsi suggérées, l'on étudie des exemples de canaux pour lesquels l'amélioration par rapport aux schémas de codage existants est nette et stricte.

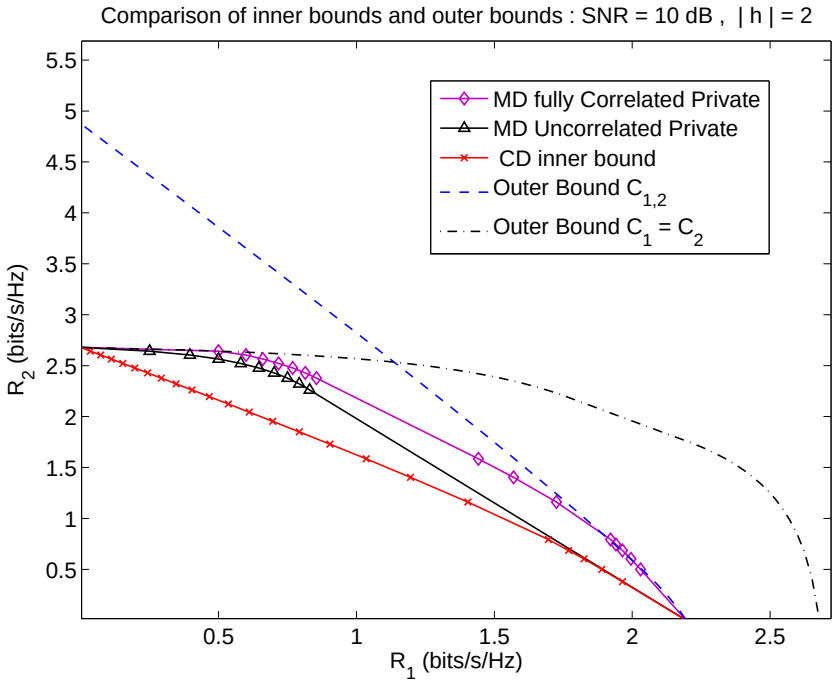


Figure 2: Comparison of the inner bounds and the intersection of the outer bounds: SNR = 10 dB, $\|\mathbf{h}_1\| = \|\mathbf{h}_2\| = 2$.

Chapitre Second: Canaux à interférences cognitifs avec transmissions multiples

1 Introduction

Le canal à interférences cognitif a été introduit pour la première fois par Devroye et.al [6] comme étant un canal à interférences avec deux sources et deux utilisateurs mais où l'une des deux sources (cognitive) a une connaissance apriori du message de l'autre source (primaire).

Les premiers résultats de capacité pour ce modèle reviennent à Maric *et.al* [7] pour le cas des interférences très fortes et à Wu [8], et Jovicic [17] pour le cas des très faibles interférences. D'autres régimes ont été totalement caractérisés dont: le canal Z [18], la classes de canaux moins bruyants[19] ainsi que la classe des canaux Plus Capables [20]. Plus tard, Rini et.al formaliseront une région de débit qui englobe toutes les régions de capacité jusque lors connues et leur permettra même de caractériser la région de capacité du canal où l'utilisateur cognitif a une meilleure prédisposition au décodage. Le cas Gaussien a été par ailleurs intensivement exploré et plusieurs régimes ont été résolus, bien que la région de capacité dans le cas le plus général reste encore un problème ouvert.

Dans cette thèse, nous étudions la classe de canaux d'interférences avec transmissions multiples où plusieurs utilisateurs primaires sont intéressés par le même message message W_1.

Nous débutons notre analyse par l'élaboration d'une borne interne à la région de capacité qui combine les codages optimaux pour le canal de diffusion (superposition de codes et random binning) et pour le canal à interférence (division de débit). Nous évaluons ensuite cette région dans les régimes de très fortes et de très faibles interférences montrant à travers des nouvelles techniques de bornes externes que les régions de débit obtenues sont optimales. Lorsque les interférences sont mixtes très faibles/ fortes, l'on a recourt à la technique de codage précédemment étudiée, le décodage de l'interférence, où l'on requiert des utilisateurs en fortes interférences de décoder l'interférence tout en empêchant les utilisateurs en faibles interférences d'en faire autant.

Commençons tout d'abord par énoncer la région de débit sur laquelle nous nous basons dans la suite.

Theorem 4. *Une borne interne à la région de capacité est donnée par toutes les paires*

de débit vérifiant:

$$R_1 \leq \min_{j\in[1:N]} I(Q_1X_1QU;Y_j) \tag{1a}$$
$$R_2 \leq I(QV;Z|Q_1) - I(QV;X_1|Q_1) \tag{1b}$$
$$R_2 \leq \min_{j\in[1:N]} I(X_1U;Y_j|Q_1Q) + I(QV;Z|Q_1) - I(V;X_1U|Q_1Q) \tag{1c}$$
$$R_2 \leq \min_{j\in[1:N]} I(X_1QU;Y_j|Q_1) + I(V;Z|Q_1Q) - I(V;X_1U|Q_1Q) \tag{1d}$$
$$R_2 \leq \min_{j\in[1:N]} I(X_1QU;Y_j|Q_1) + I(QV;Z|Q_1) - I(V;X_1U|Q_1Q) - I(Q;X_1|Q_1) \tag{1e}$$
$$R_1+R_2 \leq \min_{j\in[1:N]} I(X_1U;Y_j|Q_1Q) + I(Q_1QV;Z) - I(V;X_1U|Q_1Q) \tag{1f}$$
$$R_1+R_2 \leq \min_{j\in[1:N]} I(Q_1X_1QU;Y_j) + I(V;Z|Q_1Q) - I(V;X_1U|Q_1Q) \tag{1g}$$
$$R_1+R_2 \leq \min_{j\in[1:N]} I(Q_1X_1QU;Y_j) + I(QV;Z|Q_1) - I(V;X_1U|Q_1Q) - I(Q;X_1|Q_1) \tag{1h}$$
$$R_1+R_2 \leq \min_{j\in[1:N]} I(X_1QU;Y_j|Q_1) + I(Q_1QV;Z) - I(V;X_1U|Q_1Q) - I(Q;X_1|Q_1) \tag{1i}$$
$$R_1+2R_2 \leq \min_{j\in[1:N]} I(X_1QU;Y_j|Q_1) + I(Q_1QV;Z) + I(V;Z|Q_1Q) - I(V;X_1U|Q_1Q) - I(Q;X_1|Q_1) \tag{1j}$$
$$R_1+2R_2 \leq \min_{j\in[1:N]} I(Q_1X_1QU;Y_j) + I(QV;Z|Q_1) + I(V;Z|Q_1Q) - I(V;X_1U|Q_1Q) - I(Q;X_1|Q_1)\ , \tag{1k}$$

pour une loi de probabilité jointe $P_{Q_1X_1QUVX_2}$ *vérifiant* $(Q_1QUV)\multimap(X_1,X_2)\multimap(Y_1,\cdots,Y_N,Z)$

2 Résultats de capacité avec transmissions multiples

2.1 Capacité dans le régime de très fortes interférences

Dans cette partie du travail, nous calculons la région de capacité du canal à interférences cognitif avec transmissions simultanées lorsque tous les utilisateurs sont affectés par de très fortes interférences.

A cette fin, définissons tout d'abord le régime de très fortes interférences:

$$\forall P_{X_1X_2} \qquad I(X_2;Z|X_1) \leq \min_{j\in[1:N]} I(X_2;Y_j|X_1) \tag{2}$$
$$\forall P_{X_1X_2} \qquad \min_{j\in[1:N]} I(X_1X_2;Y_j) \leq I(X_1X_2;Z)\ . \tag{3}$$

Le schéma optimal dans ce cas là consiste à faire décoder à tous les utilisateurs tous les signaux utiles et l'interférence de l'utilisateur opposé.

Theorem 5 (Très fortes interférences)**.** *La région de capacité du canal à interférences cognitif avec transmission simultanée est donnée par l'ensemble des paires de débit* (R_1,R_2) *vérifiant:*

$$\begin{cases} R_2 & \leq & I(X_2;Z|X_1)\ , \\ R_1+R_2 & \leq & \min\limits_{j\in[1:N]} I(X_1X_2;Y_j)\ . \end{cases} \tag{4}$$

pour une loi jointe de probabilité (X_1,X_2)*.*

2.2 Capacité dans le régime de très faibles interférences

Le régime de très faibles est défini lorsque tous les utilisateurs sont affectés par de très faibles interférences.

$$\forall P_{UX_1X_2} \ : \ \begin{cases} \forall j \in [1:N] \quad I(U;Y_j|X_1) & \leq & I(U;Z|X_1) \ , \\ \min\limits_{j\in[1:N]} I(UX_1;Y_j) & \leq & I(UX_1;Z) \ , \end{cases} \tag{5}$$

tel que $U \multimap (X_1, X_2) \multimap (Y_1, \cdots, Y_N, Z)$.

Dans le cas d'un canal à interférences cognitif sans transmission simultanée, l'écriture d'une borne externe nécessite de recourir à l'identité de Csiszár & Körner's qui elle, empêche de manière intrinsèque l'extension des résultats à un nombre quelconques d'utilisateurs.

Par la suite, nous écrivons une borne externe à la région de capacité sans recourir à cette identité, ce qui nous permettra de caractériser la région de capacité dans le cas de transmissions multiples.

Theorem 6 (Borne externe dans le cas de faibles interférences)**.** *La région de capacité du canal à interférences cognitif lors de faibles interférences, i.e.*

$$\forall j \in [1:N] \ , \ \forall P_{UX_1X_2} \ , \quad I(U;Y_j|X_1) \leq I(U;Z|X_1) \ , \tag{6}$$

est incluse dans la région définie par:

$$\begin{cases} R_1 & \leq & \min\limits_{j\in[1:N]} I(UX_1;Y_j) \ , \\ R_2 & \leq & I(X_2;Z|X_1U) \ , \end{cases} \tag{7}$$

pour un ensembles de variables corrélées (U, X_1, X_2) telles que $U \multimap (X_1, X_2) \multimap (Z, Y_1, \cdots, Y_N)$.

La région de capacité dans le cas de très faibles interférences découle de cette borne externe et de la borne interne énoncée en début de chapitre. La stratégie optimale consiste alors à faire décoder aux utilisateurs Y leurs signaux utiles X_1 et U, tandis que l'utilisateur Z décode son signal utile X_2 ainsi que l'interférence (X_1, U).

Theorem 7 (Très faibles interférences)**.** *La région de capacité du canal à interférence cognitif avec transmission simultanée affecté par de très faibles interférences est définie par l'ensemble des paires de débit:*

$$\begin{cases} R_1 & \leq & \min\limits_{j\in[1:N]} I(X_1U;Y_j) \ , \\ R_2 & \leq & I(X_2;Z|X_1U) \ . \end{cases} \tag{8}$$

pour des variables arbitrairement corrélées (U, X_1, X_2) satisfaisant $U \multimap (X_1, X_2) \multimap (Y_1, \cdots, Y_N, Z)$.

2.3 Capacité dans le régime d'interférences mixtes

Nous nous intéressons par la suite au cas où l'ensemble des utilisateurs peut être partitionné en deux groupes: un groupe d'utilisateurs affecté par de très fortes interférences, $\mathcal{S}$, et un autre groupe $\mathcal{W}$ affecté lui par de très faibles interférences.

$$\forall j \in \mathcal{W} \quad , \quad I(U;Y_j|X_1) \leq I(U;Z|X_1) \ , \tag{9}$$

$$\forall j \in \mathcal{S} \quad , \quad I(X_2; Z|X_1) \leq I(X_2; Y_j|X_1) \ , \tag{10}$$

$$\min_{j\in\mathcal{S}} I(X_1X_2; Y_j) \leq I(X_1X_2; Z) \text{ Or } \min_{j\in\mathcal{W}} I(UX_1; Y_j) \leq I(UX_1; Z) \ . \tag{11}$$

Ainsi, la stratégie optimale que l'on peut intuiter des deux sections précédentes est de laisser l'utilisateur Z toujours décoder l'interférence (X_1, U) conjointement à son information utile X_2, alors que pour la classe d'utilisateur Y, les instances Y_j affectées par une faible interférence décodent uniquement leur signal utile: (X_1, U) et celles en fortes interférences décodent tous les signaux à l'instar de l'utilisateur Z.

La région de capacité fait donc clairement appel au principe de décodage de l'interférence que nous avons introduit en chapitre premier de cette thèse, et peut s'exprimer telle que suit.

Theorem 8 (Interférences mixtes: très fortes/faibles)**.** *La région de capacité du canal à interférences cognitifs avec transmission simultanée est donnée par l'ensemble des paires de débit vérifiant:*

$$\begin{cases} R_1 & \leq & \min\limits_{j\in\mathcal{W}} I(UX_1; Y_j) \ , \\ R_2 & \leq & I(X_2; Z|UX_1) \ , \\ R_1 + R_2 & \leq & \min\limits_{j\in\mathcal{S}} I(X_1X_2; Y_j) \ , \end{cases} \tag{12}$$

pour une loi jointe $P_{UX_1X_2}$ telle que $U \multimap (X_1, X_2) \multimap (Y_1, \cdots, Y_N, Z)$.

3 Conclusion

Afin de clore ce chapitre, nous relevons ici les principales difficultés dans les preuves des résultats de capacité dans le cas des transmissions multiples. Si la région de capacité de très fortes interférences découle naturellement de celle en l'absence de transmission simultanée, la région en très faibles interférences présente la difficulté d'écriture d'une borne externe avec plus d'une paire d'utilisateurs. Une nouvelle preuve pour la borne externe a donc du être élaborée. Dans le cas d'interférences mixtes, il s'agit plutôt d'une difficulté de codage car les différentes instances d'un même utilisateur (intéressées par le même message) doivent traiter différemment l'interférence. Ceci nous conduit à l'application du principe de décodage d'interférences précédemment étudié dans le cas des canaux de diffusion avec incertitude.

Troisième Chapitre: Canaux de diffusion avec sécurité

1 Introduction

La sécurité en théorie de l'information a été initialement introduite par Shannon dans [9] en étudiant une source qui cherche à transmettre un message à utilisateur "légitime" tout en le gardant secret par rapport à un utilisateur indésirable "espion" et où la source partage par ailleurs un clé de sécurité avec l'utilisateur légitime. Les premiers résultats sont assez pessimistes en ce qu'ils suggèrent que le débit sécurisé que l'on peut atteindre ne peut dépasser le débit de la clé de sécurité, suggérant donc que la clé de sécurité pourrait elle même être le message transmis. Ce n'est qu'avec les travaux de Wyner [2] qui a introduit la notion du canal à espion (Wiretap Channel) que l'on a pu concevoir une transmission sécurisée sans clé de sécurité. Afin de s'affranchir de la présence de l'espion, la source doit noyer le signal utile dans une séquence de bruit juste assez bruyante pour parasiter l'écoute de l'espion sans trop affecter l'utilisateur légitime. Ceci implique bien évidemment que le canal espion soit de moins bonne qualité que le canal légitime, autrement, aucun message ne peut être transmis de manière sécurisée sans une clé de sécurité privée. Csiszár & Körner's [21] généraliserons plus tard le résultat de Wyner, valable uniquement pour des canaux dégradés, à des canaux arbitraires.

Le canal de diffusion avec espion consiste en une source qui désire transmettre deux messages privés à deux utilisateurs légitimes tout en assurant leur sécurité par rapport à un noeud tiers espion. La région de capacité sécurisée de tels canaux a été étudiée par Ekrem & Ulukus dans [22] dans le cas où les canaux légitimes sont dégradés et où l'utilisateur espion a un canal plus bruité que celui des utilisateurs légitimes. Khandani a aussi par ailleurs caractérisé la région de capacité du cas Gaussien (donc dégradé) dans un travail indépendant.

Dans cette thèse, nous nous intéressons donc au même canal de diffusion avec espion et cherchons à caractériser la région de capacité dans plusieurs cas. Pour ce, nous proposons une nouvelle borne externe à la région de capacité sécurisée de tels canaux en contrecarrant les difficultés souvent rencontrées lors de l'écriture de bornes externes en présence de plus de deux terminaux. La borne externe que l'on suggère repose sur deux raisonnements distincts: le premier revient à écrire une borne en lettres simples en se basant des manipulations analytiques des bornes admissibles pour ce genre de problèmes; la suite de la preuve fait appel à une technique de réduction de variables aléatoire qui consiste à écrire une borne externe équivalent en recourant à un plus petit nombre de variables auxiliaires.

Pour ce qui est de la borne interne à la région de capacité sécurisée, nous nous basons sur une combinaison de deux techniques de codage: l'une pour le canal à espion (codage stochastique) et l'autre pour le canal à diffusion (schéma de Marton). Ces deux bornes internes et externes englobent les meilleures bornes connues jusque lors pour le canal de diffusion sans espion et généralisent tous les résultats déjà connus en la matière [22] et [23] en plus d'en fournir bon nombre d'autres résultats de capacité sécurisée. Ainsi, nous pouvons caractériser les régions de capacité sécurisée pour les canaux suivants:

1. Canal de diffusion déterministe où les deux utilisateurs légitimes observent une fonction déterministe du signal d'entrée
2. Le canal semi-déterministe où l'espion a un canal plus bruité que celui de l'utilisateur non-déterministe
3. Le canal de diffusion moins bruyant avec un espion dégradé par rapport au meilleur utilisateur légitime et plus bruité que le pire utilisateur légitime
4. Et enfin le produit de deux canaux inversement moins bruités avec un espion dégradé.

Nous illustrons aussi par là même ces résultats-ci en calculant la région de capacité sécurisée pour un exemple discret à entrée binaire et sorties binaires ou ternaires (canal binaire symétrique: BSC, et canal binaire à effacement: BEC).

2 Principales bornes à la région de capacité sécurisée

Nous donnons d'abord une borne externe à la région de capacité sécurisée du canal étudié en nous basant sur des manipulations en lettres simples extrêmement imbriquées que nous omettons par souci de clarté.

Theorem 9 (Borne externe)**.** *La région de capacité sécurisée du canal de diffusion avec noeud espion externe est donnée par l'ensemble des paires de débit vérifiant:*

$$R_1 \leq I(U_1;Y_1|TV_1) - I(U_1;Z|TV_1) \ , \tag{1}$$
$$R_1 \leq I(U_1;Y_1Y_2|TV_1V_2) - I(U_1;Z|TV_1V_2) \ , \tag{2}$$
$$R_1 \leq I(U_1;Y_1|TV_1U_2) - I(U_1;Z|TV_1U_2) \ , \tag{3}$$
$$R_1 \leq I(U_1;Y_1Y_2|TV_1U_2V_2) - I(U_1;Z|TV_1U_2V_2) \ , \tag{4}$$
$$R_2 \leq I(U_2;Y_2|TV_2) - I(U_2;Z|TV_2) \ , \tag{5}$$
$$R_2 \leq I(U_2;Y_2Y_1|TV_1V_2) - I(U_2;Z|TV_1V_2) \ , \tag{6}$$
$$R_2 \leq I(U_2;Y_2|TV_2U_1) - I(U_2;Z|TV_2U_1) \ , \tag{7}$$
$$R_2 \leq I(U_2;Y_2Y_1|TU_1V_1V_2) - I(U_2;Z|TU_1V_1V_2) \ , \tag{8}$$
$$R_1 + R_2 \leq I(X;Y_2|TZV_1) + I(U_1S_1;Y_1|TV_1) - I(U_1S_1;ZY_2|TV_1) \ , \tag{9}$$
$$R_1 + R_2 \leq I(X;Y_2|TZV_1V_2) + I(U_1S_1;Y_1Y_2|TV_1V_2) - I(U_1S_1;ZY_2|TV_1V_2) \ , \tag{10}$$
$$R_1 + R_2 \leq I(X;Y_1|TZV_2) + I(U_2S_2;Y_2|TV_2) - I(U_2S_2;ZY_1|TV_2) \ , \tag{11}$$

$$R_1 + R_2 \leq I(X; Y_1|TZV_1V_2) + I(U_2S_2; Y_2Y_1|TV_1V_2) - I(U_2S_2; ZY_1|TV_1V_2) \ , \quad (12)$$

pour une loi de probabilité jointe $P_{TV_1V_2U_1U_2S_1S_2X} = P_{TV_1V_2U_1U_2S_1S_2}P_{X|U_1U_2S_1S_2}$ *et telle que* $(T, V_1, V_2, U_1, U_2, S_1, S_2) \multimap X \multimap (Y_1, Y_2, Z)$.

Ensuite, en nous basant sur une technique de réduction de variables aléatoires, nous pouvons démontrer que la borne précédente est incluse dans celle qui suit.

Borne externe simplifiée La borne externe générale donnée précédemment est également incluse dans la région définie par:

$$R_1 \leq I(U_1; Y_1|TV_1) - I(U_1; Z|TV_1) \ , \quad (13)$$
$$R_2 \leq I(U_2; Y_2|TV_2) - I(U_2; Z|TV_2) \ , \quad (14)$$
$$R_1 + R_2 \leq I(X; Y_2|TZV_1) + I(U_1; Y_1|TV_1) - I(U_1; ZY_2|TV_1) \ , \quad (15)$$
$$R_1 + R_2 \leq I(X; Y_1|TZV_2) + I(U_2; Y_2|TV_2) - I(U_2; ZY_1|TV_2) \ , \quad (16)$$

pour une loi jointe $P_{TV_1V_2U_1U_2X}$ telle que $(T, V_1, V_2, U_1, U_2) \multimap X \multimap (Y_1, Y_2, Z)$.

Cette formulation plus simple de la borne externe sera cruciale dans la preuve converse de toutes les régions de capacité sécurisée que nous calculons.

Ensuite, basés sur les techniques standard de codage pour les canaux de diffusion (superposition de codes, binning aléatoire) et pour les canaux avec espion (codage stochastique), nous calculons une borne interne à la région de capacité sécurisée telle:

Theorem 10 (Borne interne)**.** *La région de capacité sécurisée du canal de diffusion avec espion inclus toutes les paires de débit* (R_1, R_2) *vérifiant*

$$R_1 \leq I(QU_1; Y_1|T) - I(QU_1; Z|T) \ , \quad (17)$$
$$R_2 \leq I(QU_2; Y_2|T) - I(QU_2; Z|T) \ , \quad (18)$$
$$R_1 + R_2 \leq I(U_1; Y_1|TQ) + I(QU_2; Y_2|T) - I(QU_1U_2; Z|T) - I(U_1; U_2|TQ) \ , \quad (19)$$
$$R_1 + R_2 \leq I(U_2; Y_2|TQ) + I(QU_1; Y_1|T) - I(QU_1U_2; Z|T) - I(U_1; U_2|TQ) \ , \quad (20)$$
$$R_1 + R_2 \leq I(QU_1; Y_1|T) + I(QU_2; Y_2|T) - I(QU_1U_2; Z|T) - I(U_1; U_2|TQ) - I(Q; Z|T) \ , \quad (21)$$

pour une loi jointe $P_{TQU_1U_2X}$ *telle que* $(T, Q, U_1, U_2) \multimap X \multimap (Y_1, Y_2, Z)$.

3 Capacité sécurisée pour plusieurs classes de canaux à espions

Dans cette partie, nous parcourrons l'ensemble des résultats de capacité sécurisée obtenus par une instanciation particulière de la borne interne et une preuve de converse par la borne externe que nous avons calculées.

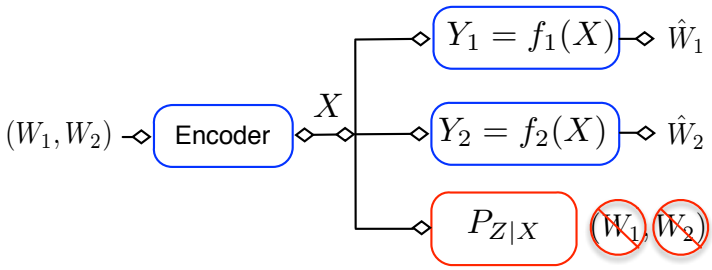


Figure 1: Canal de diffusion déterministe avec espion quelconque.

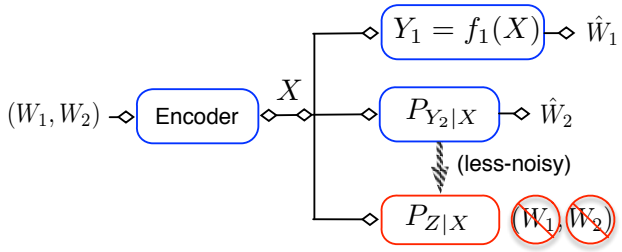


Figure 2: Canal de diffusion semi-déterministe avec espion plus bruité.

3.1 Canal de diffusion déterministe avec espion quelconque

Supposons que les deux utilisateurs légitimes observent une fonction déterministe de l'entrée du canal X, ainsi que décrit dans la Fig. 1.

Theorem 11 (Région de capacité sécurisée pour un canal de diffusion déterministe avec espion quelconque)**.** *La région de capacité sécurisée pour un canal de diffusion déterministe avec un espion arbitraire est donnée par l'ensemble des paires de débit vérifiant:*

$$R_1 \leq H(Y_1|Z) \ , \tag{22}$$
$$R_2 \leq H(Y_2|Z) \ , \tag{23}$$
$$R_1 + R_2 \leq H(Y_1Y_2|Z) \ , \tag{24}$$

pour une loi d'entrée P_X*.*

3.2 Canal de diffusion semi-déterministe avec espion plus bruité

Supposons que seul Y_1 est une fonction déterministe de X mais que Y_2 est moins bruité que la sortie Z, ainsi que décrit dans la Fig. 2.

Theorem 12 (Région de capacité sécurisée du canal de diffusion semi-déterministe avec espion plus bruité)**.** *La région de capacité sécurisée pour un canal de diffusion semi-déterministe avec un espion plus bruité est donnée par l'ensemble des paires de débit vérifiant:*

$$R_1 \leq H(Y_1|ZQ) \ , \tag{25}$$
$$R_2 \leq I(U;Y_2|Q) - I(U;Z|Q) \ , \tag{26}$$

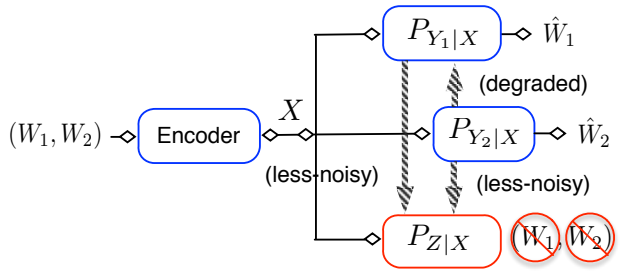


Figure 3: Canal de diffusion dégradé avec espion plus bruité.

$$R_1 + R_2 \leq H(Y_1|ZQU) + I(U;Y_2|Q) - I(U;Z|Q) \tag{27}$$

pour une loi jointe $P_{QUX} = P_Q P_{U|Q} P_{X|U}$ *telle que* $(Q,U) \multimap X \multimap (Y_1, Y_2, Z)$.

Remarks 13. *Lorsque Y_2 n'est pas moins bruité que la sortie Z, il n'est pas encore très clair si la région de sécurité peut s'écrire de manière similaire en remarquant que la variables V est inutile.*

3.3 Canal de diffusion dégradé avec espion plus bruité

Nous supposons ici que les utilisateurs légitimes sont fortement ordonnés: l'utilisateur Y_2 est dégradé par rapport à l'utilisateur Y_1.Fig. 3. Nous supposons par ailleurs que l'espion a un canal plus bruité que ceux des deux autres utilisateurs légitimes.

La région de capacité sécurisée de ce canal a été d'abord trouvée par Ekrem et Ulukus in [24], mais nous rappelons juste ici l'inclusion de ce résultat dans les régions que nous avons caractérisées.

Theorem 14 (Région de capacité sécurisée du canal de diffusion dégradé avec espion plus bruité [24])**.** *La région de capacité sécurisée du canal de diffusion dégradé avec espion plus bruité est donnée par l'ensemble des paires de débit vérifiant:*

$$R_1 \leq I(X;Y_1|TU) - I(X;Z|TU) \ , \tag{28}$$
$$R_2 \leq I(U;Y_2|T) - I(U;Z|T) \ , \tag{29}$$

pour une loi jointe P_{TUX} *telle que* $(T,U) \multimap X \multimap (Y_1, Y_2, Z)$.

Dans ce qui suit, il s'avère que la borne externe que nous avons élaborée permet aussi d'obtenir la région de capacité sécurisée d'une autre classe de canaux de diffusion ordonnés qui n'inclus pas et n'est pas incluse dans la classe de canaux de diffusion dégradés avec espion plus bruité.

3.4 Canal de diffusion moins bruyant avec espion partiellement dégradé

Supposons que le canal Y_1 est moins bruité que Y_2. En dépit de cela, nous supposons aussi que l'espion a un canal dégradé par rapport au meilleur canal légitime Y_1 tandis qu'il suffit

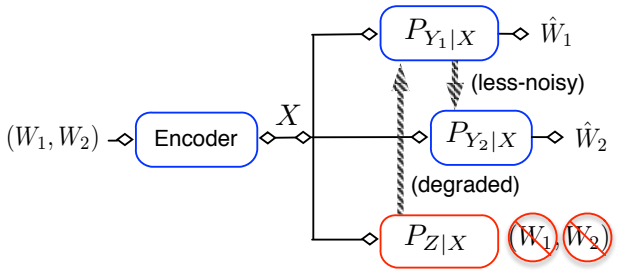


Figure 4: Canal de diffusion moins bruyant avec espion partiellement dégradé.

qu'il soit plus bruité que le second canal Y_2 ainsi que dépeint dans la Fig. 4. Ce modèle de canaux est plsu général que celui considéré par Khandani [23], mais ne généralise par forcément le travail de Ekrem et Ulukus [24].

Theorem 15 (Région de capacité sécurisée du canal de diffusion moins bruyant)**.** *La région de capacité sécurisée du canal de diffusion moins bruyant avec espion partiellement dégradé est donnée par l'ensemble des paires de débits vérifiant:*

$$R_2 \leq I(U;Y_2|T) - I(U;Z|T) \ , \tag{30}$$
$$R_1 + R_2 \leq I(X;Y_1|ZUT) + I(U;Y_2|T) - I(U;Z|T) \ , \tag{31}$$

pour une loi jointe $P_{TUX} = P_T P_{U|T} P_{X|U}$ *telle que* $(T,U) \multimap X \multimap (Y_1, Y_2, Z)$.

D'autres résultats de capacité peuvent être consultés dans le texte principal en Anglais.

4 Conclusion

Dans cette dernière partie des travaux de thèse, nous nous sommes intéressés aux canaux de diffusion avec contrainte de sécurité. Nous avons élaboré des bornes externes et internes à la région de capacité sécurisée qui se sont avérées être optimales pour bien des classes de canaux. La borne externe donnée dans ce travail constitue la principale nouveauté car ayant permis de contrecarrer les principales difficultés d'écriture de bornes externes pour les canaux à plusieurs terminaux. La borne interne suggère elle que la combinaison des techniques de codage optimales pour les réseaux de diffusion et la sécurisation des données reste la stratégie optimale à appliquer pour les réseaux de diffusion avec espion.

Main Text: Introduction

1 Preliminaries

With the uptake in broad-band mobile communications since the past decade, and in the perspective of creating fully connected environments for users to evolve in, the current and next generation networks are required to follow the trend on both supported traffic and architecture design levels.

On the one hand, future communication systems are foreseen to convey a continuously increasing traffic (voice and video streams, real time control systems, low rate data ,...). Each application dedicated traffic has to satisfy various criteria which may consist in high data rate (video applications), low latency (safety signals), high reliability (control signals), information integrity or confidentiality (secrecy), ...

On the other hand, in order for such extremely heterogeneous traffic to be accommodated through the network, the architecture as well should come as a rupture with the classical cellular systems with dedicated transmit nodes and user equipments. What the “one-works-for-all" architecture is remains subject to investigation, however, it should clearly rely on multiplying the network access points. This can be done by empowering different components of the network to act as transmit nodes, allowing thus for higher throughput and better access to information. As such, various communication scenarios such as *Broadcast*, *Multicast*, *Cognitive Interference*, *Relay* and so on, are to be encompassed within the same network as shown in Fig. 5.

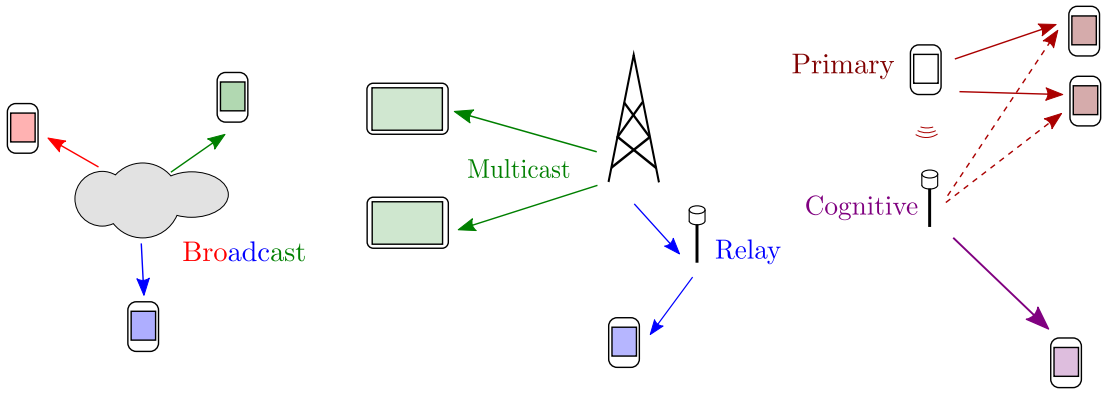


Figure 5: Basic communication scenarios in future networks.

Problematics and basic channel models

Increasing transmit and receive nodes density results in a more stringent and unstructured *interference* at local and neighbouring communication systems, all due to the open nature of the wireless medium. Mitigating interference has long been a most limiting aspect of coding for wireless networks and the optimal strategy for many interference driven channels has yet to be found. One of the most challenging communication scenarios that calls for such an efficient interference mitigation technique, be it only in the two-user case, is the *Broadcast Channel* (BC) [1]. From an information theoretic point of view, a

Broadcast channel consists in a source that wishes to transmit two distinct messages to two distinct receivers, as show in Fig. 6. The source would like to transmit individual message rates R_1 and R_2 as close to optimal as possible for each of the receivers, however, increasing the transmit rates increases the share of interference experienced by each of the receivers, and thus, a trade-off is imposed.

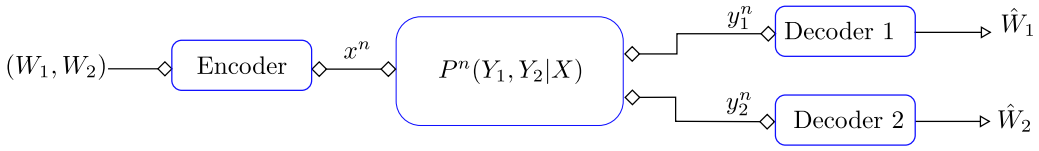


Figure 6: Standard Broadcast Channel.

Besides its vulnerability to the increasing amount of interference, the wireless medium is also subject to variable-quality links, which, alone, might degrade the communication of reliability/latency sensitive users (safety, control in electric plants, ...). When coupled with increased interference, the effect of this *channel uncertainty* becomes even more critical since most interference mitigation techniques rely on perfect knowledge of the channel statistics. From a theoretic point of view, we represent the channel statistics by a *state*. The amount of *state information* available at the source and its variability define many classes of state dependent channels: *Compound channels*, *Composite channels*, *Arbitrarily Varying channels*, ...[1]

The Compound Broadcast Channel: In this thesis, we first investigate broadcast transmissions under channel uncertainty, described by the class of *Compound Broadcast Channels*. In such a scenario, the source is oblivious to the actual channel probability distribution, however, this probability is fixed throughout the transmission and assumed to belong to a finite set of *possible* channel statistics. This setting models all *Block Fading Broadcast* channels where the channel gains are assumed to remain constant throughout the transmission but are unknown to the source. Dealing with interference in such an uncertain medium becomes even more challenging and is thus worthy of investigation.

Bearing in mind that when the source is oblivious to the channel realization, imposing that the messages be decoded whatever the channel statistics constrains the source to code for all possible channels at once as if they were all present in a multicast fashion. Hence, the Compound channel is often referred to as a multiple user channel with a common message, i.e a *Multicast* channel. This equivalence leads us to the second channel model we will be investigating in the sequel.

The Multicast Cognitive Interference Channel: Another class of interference driven channels that indeed can be affected by *multicasting* is modelled by the *Cognitive Interference Channel* (CIFC). The Cognitive Interference Channel, shown in Fig. 2, can be encountered in cognitive radio environments where a *secondary* transmitter/receiver

[1] At the source, the channel uncertainty is more hindering since, in general, the codebook construction and thus the decoding strategy depend on the prior knowledge of the channel probability at the source, and since it is also possible to learn the channel at the decoders by dedicating a tiny part of the transmission rates to this end.

pair is communicating at the same time as a *legacy primary* transmitter/receiver pair of users. The secondary source has access to the message sent by the primary source,

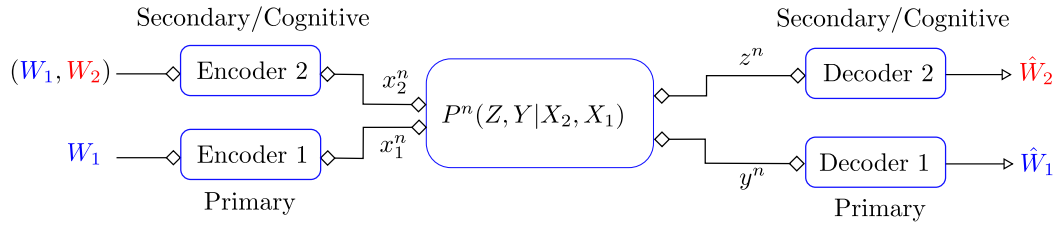


Figure 7: The Cognitive Interference Channel / Broadcast Channel with a helper.

thus it is called a *cognitive source*. Though this setting seems similar to an *interference channel* but with a cognitive source, it can be considered also as a Broadcast Channel with a helper, the helper being the primary source. The helper, upon enhancing the communication of message W_1 creates interference at user 2 that is interested only in W_2 and thus, a trade-off is imposed on the transmitted rate pairs. This trade-off is even more stringent as we increase the number of primary users and the *Mutlicast Cognitive Interference Channel* describes exactly such a setting. Such a communication scenario can be encountered, for instance, in stadiums with a signal multicast to all supporters on their receive devices while a nearby base station helps with the communication. Our aim is to determine the most effective interference mitigation technique to apply when many primary users are decoding the same message, especially as we show later, when each user experiences a different interference structure.

The Wiretap Broadcast Channel: Due again to the open nature of the wireless medium, multiplying the network access points results in challenging physical layer security issues concerning integrity and confidentiality of information. By physical layer security, we mean all strategies applied at the physical layer which ensure *safe* transmission of information in the presence of an eavesdropper, without resorting to enciphering at higher layers of the communication protocol stack. In practical systems, a communication scenario can be threatened by either an active or a passive eavesdropper. An active eavesdropper could be a jamming device trying to affect the information *integrity*, while a passive eavesdropper could be a hacker or a non-legacy user of some service compromising the *confidentiality* of information. In order for a transmission to be successful, it has to provide for rates which are both *reliable* for the legitimate receivers and *secret* to the eavesdropper. Such a trade-off is theoretically modelled by the *Wiretap* [2] channel where a source wishes to transmit a message to a legitimate receiver whilst keeping it secret from an external eavesdropper, see Fig. 8.

In this thesis, we thus study a class of Broadcast Channels with an eavesdropper that we denote by the *Wiretap Broadcast Channel* (WBC). Coding reliably (mitigating interference) and safely (securing information) for such a setting presents the advantage of not being alterable by eavesdroppers since it is set regardless of the computational and jamming power of the eavesdropper. However it can not always be ensured since depending on the physical properties of the legitimate users' and eavesdropper's channels

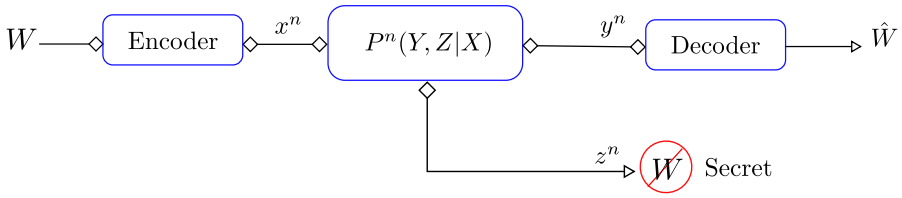


Figure 8: The Wiretap Channel.

as we clarify later on.

Methodology

The aim of the first and second parts of this thesis is to characterize the *capacity region* of the Compound BC and the Multicast CIFC which involve interference and channel uncertainty, or multicasting, based on an information theoretic approach. This approach [25] is twofold: it consists in deriving the set of rate-tuples that can be achieved with arbitrarily small probability of error under a specific random code argument (inner bound on the capacity region). It also consists in deriving the set of rate-tuples that, when exceeded, lead to a non-zero probability of error (outer bounding techniques). When an inner and an outer bound coincide for a channel model, we claim that the capacity region is fully characterized.

In the last part of this thesis, we characterize the *secrecy capacity region* of the Wiretap BC based on an information theoretic secrecy argument [9]. Besides being achievable with an arbitrarily small probability of error (reliability condition), any rate pair that lies in the secrecy capacity region should also allow for maximal equivocation – remaining uncertainty about the message – at the eavesdropper (secrecy condition). Similarly, any rates achievable with arbitrarily small probability of error and maximal equivocation at the eavesdropper should lie inside the secrecy capacity region.

In the sequel, we introduce more thoroughly the channel models we investigate and the main results we derive in this thesis.

2 The Compound Broadcast Channel

We define the M by N Compound BC as follows: a source wishes to transmit two messages (W_1, W_2) to two users Y and Z, as shown in Fig. 9, but the channel Y can equal one of many N channel instances, while Z lies in a set containing M channel instances.

As argued previously, coding successfully for this channel requires an interference mitigation technique robust to channel uncertainty. To construct alternative coding schemes, one has thus to understand the effect of the coupling between channel uncertainty and interference. In the sequel, we give intuitive examples of BCs which, when plagued with channel uncertainty, require more evolved coding schemes than the existing ones and we explain therefore how to palliate channel uncertainty.

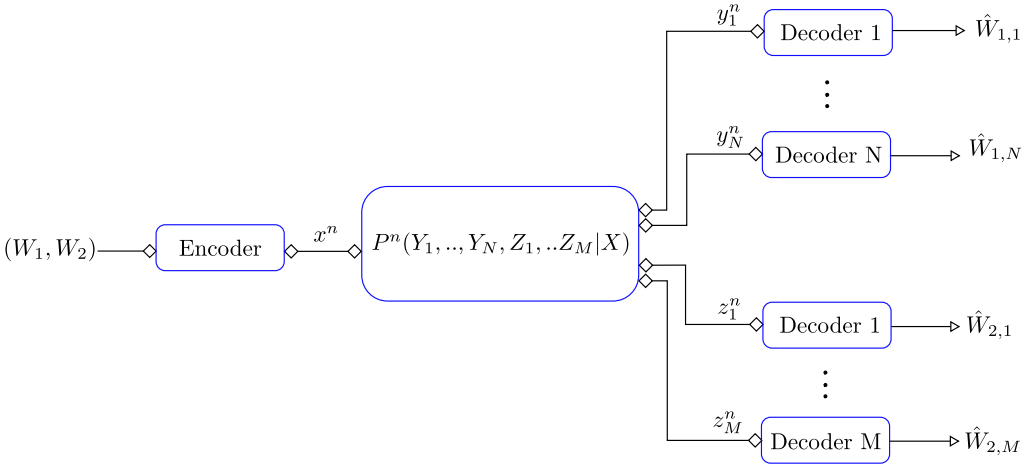


Figure 9: The N by M Compound BC / N by M multi-user BC with two common messages.

2.1 Ordered Compound BCs

A very simple yet insightful example of an ordered BC for which channel uncertainty at the source can bring about severe loss, is the degraded BC where the two receivers Y and Z are ordered in terms of channel quality, and thus, in terms of decoding capabilities. The optimal interference mitigation technique in such a standard –non compound– setting, is for the source to transmit two layers of codewords. Upon a *common* layer that is aimed to be decoded at both users, a *private* layer is superimposed and intended to be decoded only at the stronger user, say Y. The resulting capacity region of such a setting is given by the set of rate pairs that satisfy:

$$\begin{cases} R_1 & \leq & I(X;Y|V) \\ R_2 & \leq & I(V;Z) \end{cases} \tag{32}$$

for some common auxiliary random variable that verifies the following Markov chain $V \multimap X \multimap (Y, Z)$. This scheme is very sensitive to the users' ordering, and thus, requires both users and the source to implement the right *superposition* (encoding and decoding) strategies to achieve the capacity region.

In the Compound BC setting, where the source and decoders might fail to *guess* the right encoding/decoding order, applying the inverse superposition coding scheme can not outperform the mere Time Sharing scheme as it is shown in Fig. 10 for a Gaussian example.

To bypass this limitation, we resort in Chapter 1 to the idea of *Interference Decoding (ID)* where, basically, relying on a completely symmetric encoding scheme – Marton's random coding scheme [3]– and by allowing each receiver to decode/or not the interfering message of the other user, we recover all possible superposition-coding-like rate regions. This strategy thus finds its full utility, for instance, in a 2 by 1 Compound BC where the two possible channels of the same user Y_1 and Y_2 might require the use of two inverse decoding strategies since inversely ordered towards the user's output Z.

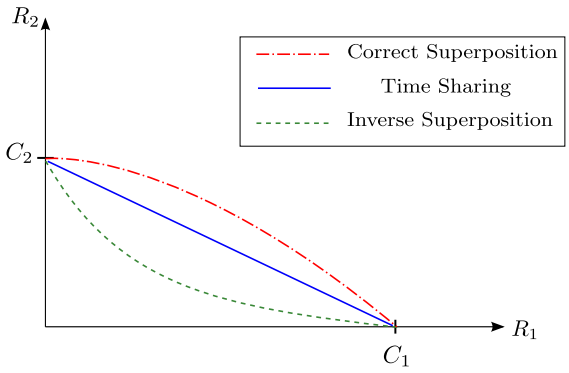


Figure 10: Comparison of superposition schemes for a Gaussian BC.

However, to identify practical classes of compound channels for which Interference Decoding scheme strictly outperforms the *Non Interference Decoding* (NID) scheme, i.e Marton's inner bound in its worst case channels formulation, a full understanding of the effect of the coupling of channel uncertainty and interference had to be carried out. It turned out that, for most ordered channels for which capacity is known (e.g AWGN BC, Binary Symmetric BC, Binary Erasure BC), the compound setting reduces inevitably to a standard BC formed by the two *worst* instances among the two groups of users, mostly due to stochastic and physical degradedness [4].

This results from the fact that applying the wrong decoding strategy at the best channel instance of a user does not impede the communication, since the only bottleneck of the transmission rates is the poor quality of the other channel instances. Fig. 11 illustrates such a fact for the 2 by 1 Compound Gaussian BC where Z is degraded with respect to Y_1, while Y_2 is degraded with respect to Z. Hence, applying the right encoding/decoding strategy for the "worst pair" BC, i.e (Y_2, Z), is capacity achieving.

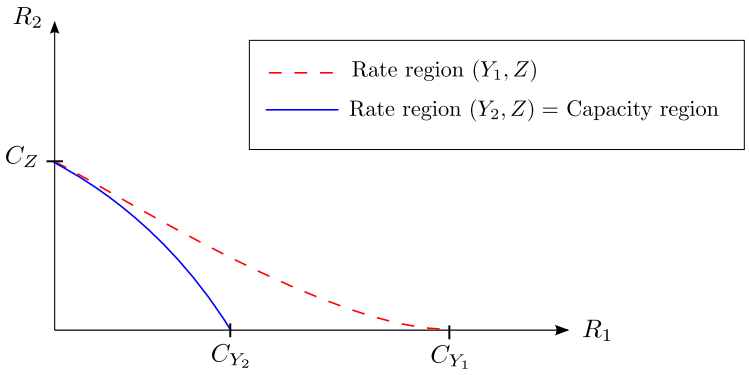


Figure 11: An irrelevant Compound Broadcast Channel.

This could be explained more thoroughly by the fact that Interference Decoding for the standard 1 by 1 BC does not improve over Maton's inner bound since the latter already includes all superposition coding schemes due to the combination between Superposition

Coding and Random Binning. Thus, whenever a class of Compound BCs reduces to a single Broadcast Channel, resorting to ID is of little use if none.

Contribution In Chapter 1 of this thesis, we investigate the role that ID can play in ordered Compound BCs. Upon characterizing such *trivially* ordered Broadcast settings, for which ID can not be expected to be of much enhancement to the communication rates, we identify a class of relevant 2 by 1 Compound BCs. This class allows for antagonist orderings between the different BCs (Y_1, Z) and (Y_2, Z) and thus requires antagonist decoding rules at each instance of the compound setting. In this case, the gain of Interference Decoding is manifest and can be proved.

2.2 Non ordered Compound BCs

When the BC components do not exhibit any form of order, then, unlike ordered BC where there is a need to *decode interference*, the best strategy to deal with interference is to *precode against it at the source*, resorting to random binning. An achievable rate region when the interferences V, resp. U, is pre-cancelled at the source [3] is given by $\mathcal{R}_1$, resp. $\mathcal{R}_2$:

$$\mathcal{R}_1 \ : \ \left\{ \begin{array}{rcl} R_1 & \leq & I(U;Y) - I(U;V) \ , \\ R_2 & \leq & I(V;Z) \ , \end{array} \right. \quad \mathcal{R}_2 \ : \ \left\{ \begin{array}{rcl} R_1 & \leq & I(U;Y) \ , \\ R_2 & \leq & I(V;Z) - I(U;V) \ . \end{array} \right.$$

where the two auxiliary random variables U and V satisfy the Markov chain: $(U, V) \multimap X \multimap (Y, Z)$.

One maybe of the most well known classes of BCs for which this strategy is optimal, is the Multiple Input Multiple Output (MIMO) BC, where capacity is achieved resorting to Costa's Dirty Paper Coding (DPC) [16] to cancel, in turns, the interference of both users [5]. The capacity region is obtained thus letting $U = X_u + \alpha V$ and $X = X_u + V$ where α is a parameter that needs to be tuned and that depends on the actual MIMO channel Matrix and noise powers. Again, if the source were to be oblivious of such information, then the performance of the wrong DPC choice is but optimal and its performance is far from being optimal as SNRs grow higher (DoF analysis). Fig. 12 illustrates the resulting loss.

To palliate this limitation, we introduce in Chapter 2 the idea of *Multiple Description* coding which consists in generating, in spite of a common description that is to be decoded at all instances, many distinct descriptions, decoded each at an instance of channels. These private descriptions accommodate differently the information since they precode against interference using each an optimal DPC parameter for the intended channel instance. As such, they enhance the single rates achieved by each of the instances compared to the rates achieved by a common DPC parameter for all channels of the same user. However, as it is custom in sending correlated signals over channels, this results in a loss tantamount to the correlation cost between the *private descriptions* and hence, a compromise has to be found.

Here, we notice that when interference and uncertainty are not coupled, e.g Standard

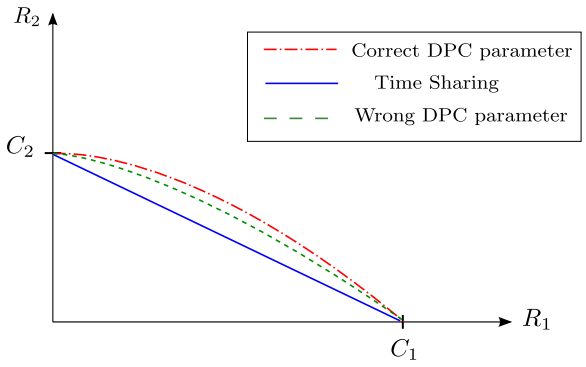


Figure 12: Comparison of DPC schemes for a MISO BC.

non compound BC or Compound Point-to-Point channel, then MD coding does not enhance the performance of CD coding, i.e Marton's inner bound. However, when both are coupled, the gain is consequent and we illustrate it for a class of 2 by 1 Compound MISO BC, that is naturally relevant unless both channels Y_1 and Y_2 are collinear.

Contribution The main outcome of Chapter 2 of the thesis is hence that, since resorting only to a common DPC imposes a very stringent trade-off on the optimal common parameter α, the communication performance can be enhanced by resorting to both a common DPC and dedicated private DPCs tuned each to be aligned for a distinct channel instance. Upon observing that the resulting loss from the correlation of the private DPCs causes less impediment than improvement to the transmitted rates, we further notice that MD coding enhances the communication rates even more when the channels of the same user are close to being orthogonal, i.e when the trade-off imposed on the common DPC parameter is most stringent.

3 The Multicast Cognitive Interference Channel

Another interesting setting that arises from the new generation architecture, is the Cognitive Interference Channel as first introduced by Devroye *et.al* [6] to model an Interference Channel (IFC) with a cognitive source that has access to both messages to be transmitted. This setting could also model other communication scenarios and thus is investigated in literature under different appellations: the *Interference Channel with Unilateral Transmitter Cooperation*, the *Interference Channel with Degraded Message Sets* at the sources, as well as the class of *Broadcast Channels with a helper*.

The CIFC encompasses three basic communication scenarios, thus coding optimally for such a setting implies combining the optimal coding schemes for each of these components: superposition coding and random binning to convey information through the BC setting defined by: $X_2 \to (Y, Z)$, rate splitting to convey information over the Interference Channel (IFC) $(X_1, X_2) \to (Y, Z)$ and finally, correlating inputs X_1 and X_2 to transmit information over the Multiple Access Channel $(X_1, X_2) \to Y$.

Though the capacity region of this setting is not fully characterized, it is quite well

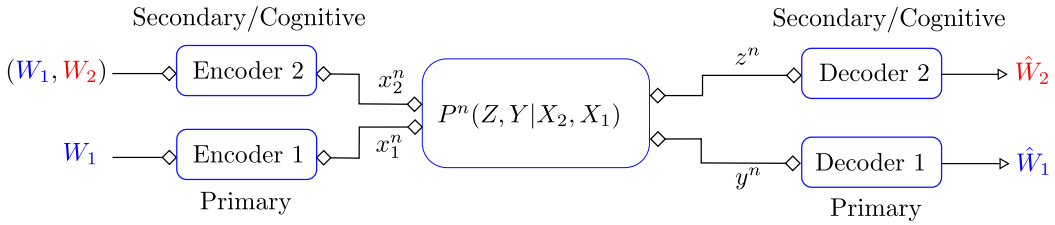


Figure 13: The Cognitive Interference Channel.

understood for many ranges of interference. For the *very strong interference* regime, the optimal strategy is to let both decoders decode interference, yielding thus a capacity region of the form [7]:

$$\begin{cases} R_2 & \leq & I(X_2; Z|X_1) \\ R_1 + R_2 & \leq & I(X_1 X_2; Y) \ . \end{cases} \tag{33}$$

For *very weak interference* and *primary better than cognitive*, what is optimal is to let the cognitive decoder decode all signals while the primary receiver considers interference of the secondary transmission as noise (see [26] and [8]) which results in:

$$\begin{cases} R_1 & \leq & I(UX_1; Y) \\ R_2 & \leq & I(X_2; Z|UX_1) \ . \end{cases} \tag{34}$$

Yet, these interference mitigation strategies depend strongly on the respective channel statistics Y and Z, and hence, when many users are interested in the same message, coding optimally for all possible channels requires that the source account for all possible interference regimes at once, and thus, requires more evolved schemes than a naive common coding argument.

Thus, in Chapter 3 of this thesis, we investigate the Multicast CIFC where many primary users are interested in the message W_1. Our aim is to characterize the capacity region in such a multicast setting when users experience each a given interference: very strong interference, very weak interference, ...

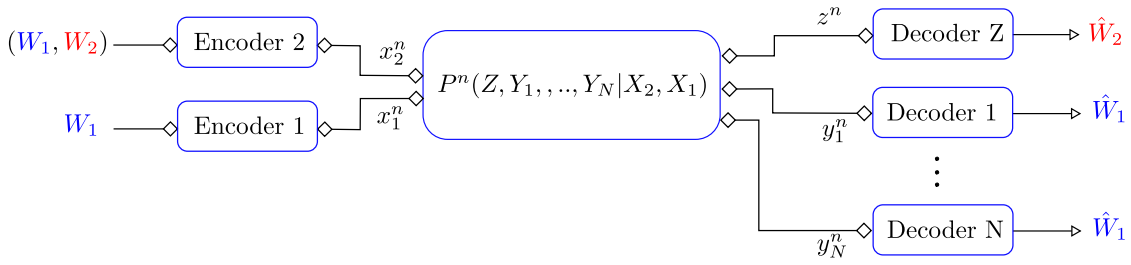


Figure 14: The Multicast Cognitive Interference Channel / Broadcast Channel with a helper and a common message.

Contribution The main outcome of this work is that the optimal strategies in very strong and very weak interference, stay optimal with an arbitrarily number of users. The

intuition suggests that, if all primary users are in strong interference regime, they all can decode interference and so can the secondary receiver. Else, if all primary users experience very weak interference, it is optimal that all of them consider interference of the secondary source X_2 as noise. Yet, the most challenging part of the work, is to characterize the capacity region for those settings where users can be split in two groups: a group that experiences very weak interference, and a group that experiences very strong interference. The capacity region in this mixed weak strong interference case is achieved through a careful combination of optimal schemes for both groups of users. We report likewise the capacity of the corresponding Gaussian examples resorting to these optimal encoding techniques, evaluating the inner bound with a specific Gaussian code construction, along with standard Gaussian upper bounding theorems.

4 The Wiretap Broadcast Channel

Information theoretic secrecy was first introduced by Shannon in the seminal work [9] where he investigates a communication system between a source, a *legitimate* receiver and an *eavesdropper* and where the source and the legitimate receiver share a secret key through a dedicated secret link. The rather pessimistic result of Shannon's work is that, to achieve perfect secrecy, one has to let the key be at least of the same length as the message; one could then rather transmit the message directly through the secret link. This result motivated the work [2] by Wyner who introduced the notion of Wiretap Channel.

In such a setting, a source wishes to transmit a message to a *legitimate* receiver in the presence of an *eavesdropper* but without resorting to a shared key. Besides communicating reliably to the legitimate receiver at a maximum rate, the source has to maximize the equivocation at the eavesdropper, i.e $\frac{1}{n}H(W|Z^n)$, meaning it can recover but a part of the transmitted message.

In the case of perfect secrecy, the conditional probability of the message given the eavesdropper's observation has to be approximately uniform over the set of messages, i.e. $\lim_{n\to\infty} \frac{1}{n}H(W|Z^n) = R$, there is no leakage of information to the eavesdropper. The surprising result of Wyner's work [2] is that the use of a secret key is no longer required to guarantee a positive equivocation rate or even perfect secrecy.

The Wiretap Channel captures very well the tradeoff between reliability of transmission, which would require to send rates low enough to enable a correct decoding at the legitimate user, and secrecy, which would require sending rates high enough so as not to be decoded by the eavesdropper. The optimal strategy to achieve such a secrecy without resorting to a shared secret key, lies in the idea of stochastic encoding, where the source dumps the useful signal in a noise sequence making it impossible for the eavesdropper to decode information, but ensuring that the noise level is low enough to enable the legitimate decoder recover its message. The secrecy capacity is thus given as:

$$C_s = \sup_{P_{UX}} [I(U;Y) - I(U;Z)] \tag{35}$$

As one can notice, this requires implicitly that the legitimate user have a *better* channel

than the eavesdropper which is a natural constraint since no physical layer security can be achieved (in the absence of a shared key) if the eavesdropper has a better decoding capability than the legitimate user.

In the last part of this thesis, we investigate the Wiretap Broadcast Channel shown in Fig. 15 where a source wishes to send a pair of messages, each to a legitimate receiver, whilst keeping them secret from an external eavesdropper.

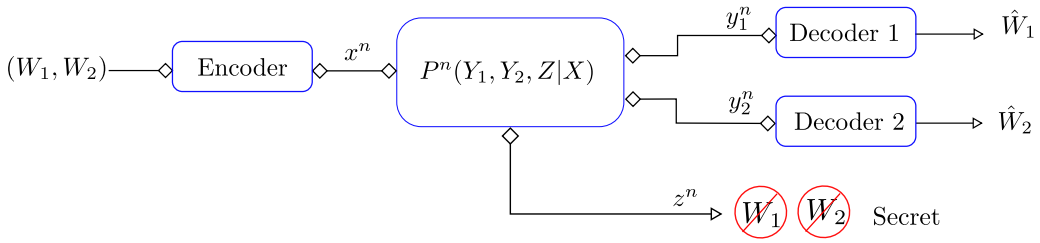


Figure 15: The Wiretap Broadcast Channel.

Our aim is to infer the best strategy to apply in such a Broadcast setting, combining the best coding scheme of the Broadcast channel with the idea of stochastic encoding. The idea behind the encoding part is that to secure both messages, it is not enough to ensure that each of them is secure, rather, it is crucial that both be jointly secure, which would imply individual secrecies.

$$\lim_{n\to\infty} \frac{1}{n} H(W_1 W_2 | Z^n) = R_1 + R_2. \tag{36}$$

Thus, based on Marton's inner bound for the BC, we let each of the two private codewords in the code construction secure independently its dedicated message, however, both should then secure jointly the two messages. This yields an inner bound that contains all previous known results for the WBC.

Contribution Yet, the main theoretic gap to be filled is, without a doubt, the outer bounds which difficulty arises from the limitation of currently existing tools to encompass more than 2 channel outputs. To palliate this difficulty, in Chapter 4 we rely on a two steps outer bounding technique. First, based on the standard Fano's inequality and secrecy requirement (36), we can derive a novel single letter outer bound on the secrecy capacity region of a general WBC that requires some non trivial analytic manipulations. Then, we give an equivalent formulation of the outer bound through the simplification of some auxiliary random variables that prove to be useless when optimizing over all input probability distributions. Based on this outer bound, we can fully characterize the secrecy capacity region of some classes of Wiretap Broadcast Channels that had long remained unstudied.

Abbreviations

Throughout this thesis, we use the following abbreviations:

Abbreviation	**Expression**
pmf	probability mass function
rv	random variable
LLN	Law of Large Numbers
EPI	Entropy Power Inequality
FME	Fourrier-Motzkin elimination
BC	Broadcast Channel
CIFC	Cognitive Interference channel
WBC	Wiretap Broadcast channel
ID	Interference Decoding
NID	Non Interference Decoding
MD	Multiple Description
CD	Common Description
DPC	Dirty Paper coding
BEC	Binary Erasure channel
BSC	Binary symmetric channel
MISO	Multiple Input Single Output
SNR	Signal to Noise Ratio
VWI	Very Weal Interference
VSI	Very Strong Interference
BCD	Better Cognitive Decoding

Notations

We resort to some well known operators and functions denoted as follows:

Notation	Definition
$H(\cdot)$	Entropy
$I(\cdot;\cdot)$	Mutual Information
$H_2(\cdot)$	Binary entropy function $H_2(x) \triangleq -x\log_2(x) - (1-x)\log_2(1-x)$
$h(\cdot)$	Differential entropy
$\mathbb{E}$	Expectation
$\mathbb{P}$	Generic Probability
P	pmf of a random variable
$\mathbb{1}$	Indicator function
$\|\mathcal{X}\|$	Cardinality of the set $\mathcal{X}$
x_k^n	The collection $(x_k, \ldots, x_n)$
x^n	The entire sequence $(x_1, \ldots, x_n)$
$T_\delta^n(X)$	The typical sets of P_X (see Appendix A for details)
$T_\delta^n(Y\|x^n)$	The conditional typical set of $P_{Y\|x^n}$
$\preccurlyeq$	Less noisiness
$x \star y$	Binary convolution operator $x \star y \triangleq x(1-y) + (1-x)y$
$\mathbf{h}^t$	The transpose of the real-valued vector $\mathbf{h}$

Also, the following conventions apply:

- Random variables and their realizations are denoted by upper resp. to lower case letters.
- Vectors are denoted by bold font characters.
- Let X, Y and Z be three RVs on some alphabets with probability distribution p. If $p(x|yz) = p(x|y)$ for each x, y, z, then they form a Markov chain, which is denoted by $X \multimap Y \multimap Z$.
- Let $\mathbf{B}_u$ $\mathbf{h}_j$ and be unit-norm 2×1 column vectors. We denote the scalar product between vectors $\mathbf{B}_u$ and $\mathbf{h}_j$ by $h_{j,u} = \mathbf{h}_j^t \mathbf{B}_u$.

Part I

The Compound Broadcast Channel

Introduction and Setup

1 Introduction

The two-user Broadcast Channel –as first introduced by Cover in [1]– consists of an encoder transmitting two private messages to two users, see Fig. 6.

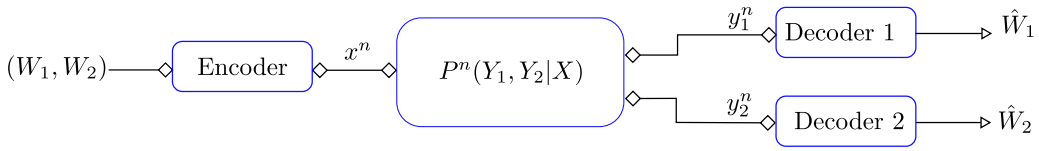


Figure 1: Standard Broadcast Channel.

Following this seminal work, intensive research was undertaken to characterize the capacity region of this setting for which the key feature in designing optimal codes is to allow for an efficient interference mitigation. In this work, we study the general two-user Compound BC where an encoder wishes to communicate two private messages to two users who can each observe one of many output channel statistics. The actual channel controlling the communication is unknown at the transmit side but assumed to remain constant during the communication and belongs to a known set of possible channels. Coding successfully for such a setting requires that the encoder must guarantee –whatever the channel realizations– reliable communication. Thus, it is well understood that the compound BC is equivalent to a BC with multiple users and common information. Our aim is to improve the understanding of how interference should be dealt within the current setting where both channel uncertainty and interference are coupled. To this end, we study alternative encoding and decoding techniques to the usual coding schemes that were proved to be capacity achieving for some broadcast channels.

Let us first briefly discuss the optimal coding schemes for the two-user BC, reported also partly in [27]. Although the capacity region of the BC still remains an open problem to this day, Marton established in [3] an inner bound on the general two-user BC based on the notion of *random binning* and *superposition coding* with common and private messages, commonly referred to as "Marton's coding". This inner bound remains the best hitherto known in literature while the best outer bound on the capacity region of the BC is due to Nair & El Gamal [28]. These two bounds were shown to coincide for several classes of "ordered" channels, citing here: degraded, less noisy, and more capable BCs (see [10] and references therein) and more recently [29], for essentially less noisy and essentially more capable BCs, the key feature being the use of *superposition coding* as an

encoding strategy. Marton's inner bound also proved to be capacity-achieving for some non-ordered channels: the deterministic and semi-deterministic BC in [3] and [11], the MIMO BC in [5] while the capacity region of a BC consisting of the product and sum of two unmatched channels is also reported in [12]. In these cases, it is *random binning* that proves to be crucial for interference management.

In the above mentioned works, the channel statistics are perfectly known to the transmitter and thus the encoder can exploit this knowledge to allow for an efficient interference mitigation scheme. In all the cases where Marton's inner bound is tight, the construction of the optimizing auxiliary code depends on the prior knowledge of either the channel output statistics (e.g. deterministic and semi-deterministic BCs) or a function of these statistics (e.g. users' ordering in ordered single antennas BCs). When the encoder is oblivious to any such information about the channel state –no channel state information (CSIT)–, the effect of interference coupled with channel uncertainty on Marton's coding technique can be more stringent. This brings about the necessity to explore encoding and decoding schemes that are powerful enough to deal with the effects of channel uncertainty.

1.1 Related Work

It is worth mentioning here that few works dealt lately with alternate decoding techniques. We cite here first [30], where the authors characterized the maximum rate region for general interference networks under a given code constraint. This work generalizes the technique of "Interference Decoding" (ID), which was already used in [14], and consists in an alternate strategy for treating interference at receive terminals. More precisely, ID combines *non-unique decoding* with the possibility at each receiver to decode or not the interfering messages intended to the others users. As a matter of fact, the gain of ID does not result from non-unique decoding [31] as much as it follows from decoding interference. Yet, the straight-forward extension of the results of this work [30] to the BC is not strong enough for it encompasses only *superposition coding* but not *random binning*. Nevertheless, it provides an interesting insight on how to recover a *superposition coding* like inner bound with alternative decoding strategies, while keeping a symmetric encoding which will be useful for ordered channels.

Later, authors in [32] derived an inner bound based on "Coset Codes" for the three users BC possibly enlarging the best-known known inner bound. Coset codes are *structured codes* that allow the destinations to decode a "compressive" function of the interfering messages and thus a complete cancellation of interference with less impediment to the information rates than fully decoding the interfering messages. A class of 3 users BCs is proposed where two links are interference free and for which the straightforward extension of Marton's coding scheme, stays strictly suboptimal compared to the suggested rate region. Such a coding technique based on Coset Codes, proves to be useful for three user BC, however, it does not enlarge Marton's inner bound in the two user's case. Yet this work presents the first class of 3 users BC for which Marton's inner bound, with many common layers, is strictly sub-optimal.

When the channels are not ordered, e.g, MISO BC, the effect of channel uncertainty on the "Degrees of Freedom" (DoF) –insightful to understand how interference should be managed with no CSIT– is rather well understood. For finite state compound settings,

Weingarten *et al.* had first derived both inner and outer bounds on the DoF region and on the sum-DoF of the compound MISO BC [33] with some cases of optimality. The outer bound derived therein was conjectured to be loose, but later Gou *et.al* [34] and Maddah-Ali [35] proved the optimal DoF region of the generic compound MISO BC, both in the complex and in the real settings, to perfectly match this outer bound. The achievability of the optimal DoF relies on either a Linear or a non-Linear coding scheme combined with "symbol extensions" in [33] while the proof made in [35] resorts to number theory tools and consists in interference alignment over rational dimensions of the real numbers (see also [36]). When the states span an infinite set, i.e., in the ergodic setting, DoF can experience severe loss. In [37], it is shown that with Rayleigh fading channels, the sum-DoF collapses to the number of transmit antennas: time-sharing is optimal. A few more works deal with alternate settings where various models of the amount and accuracy of CSI available at the transmitter are considered, e.g. [38]. It turns out that richer encoding strategies, like *Interference Alignment* (IA) along with block expansion (coding over many time slots) are crucial in dealing with interference, and thus, any optimal scheme for the finite power limited MISO BC should encompass such coding strategies. Yet, very few capacity results are known for the compound BC, among which we can cite the capacity of a class of degraded compound MIMO BC due to Weingarten *et.al* where a specific order is imposed on the channels of the two users: [39], and more recently in [40].

1.2 Our Contribution

In this work, we explore the role that two main interference mitigation techniques can play in the compound BC setup, and show that, by operating clever optimization either on the encoding or on the decoding side, we can alleviate the effect of uncertainty when coupled with interference in two different ways. We first start by deriving a rate region that takes advantage of the combination of each of ID, Marton's *random binning*, and *superposition coding*. We prove that for the compound BC –unlike the standard two-user BC– ID can strictly outperform its antagonist "simpler" strategy, i.e., "Non Interference Decoding" (NID). The gain is due to the fact that ID allows for a symmetric encoding, and thus deals better with the source's uncertainty while relegating the "clever decoding" to the receive terminals. To illustrate clearly the role of this decoding, we investigate a class of discrete ordered compound BCs for which this improvement is strict and where ID is crucial to recreate superposition-coding like rate regions without specifying prior coding hierarchy and decoding orders.

However, if the channels are not ordered, then the ID gain is less explicit, and thus, more involved encoding schemes need to be investigated. For this reason, we look at the role that "Multiple Description" (MD) coding can play in the non-ordered compound BC, where we allow each possible instance of the same user to decode a "private description" unintended for the other channels instances. We follow a similar approach to that in [41] where MD coding had been already proved to be useful over compound state-dependent channels. Such a scheme allows the encoder to treat differently the many channel instances of each user, and the resulting decoding constraints are therefore less stringent than the "Common Description" (CD) coding scheme [3]. Indeed, the introduction of several private descriptions results in a cost tantamount to their overall correlation. Therefore,

the primary question that we aim to address here is whether this correlation is more harmful than the channel uncertainty. Our answer is mostly negative and this is stated by a class of compound MISO BC where we show that, under a specific "Dirty-Paper Coding" (DPC) scheme [16], MD coding can strictly outperform CD coding. By using a fraction of the power intended to superimpose private descriptions, each aligned for an instance of each user, can be strictly useful.

2 Problem Definition

The N by M Compound Broadcast Channel model consists in one source terminal and two distinct receivers each observing one of many possible channel outputs. The source wishes to communicate two private messages each intended to a receiver. This setting is equivalent, from a maximum probability of error, to a setting where each user is represented by multiple users each interested in the same message. A transmission scheme is said to be successful if all users and each can decode their intended messages, i.e the maximum probability of error over all terminals is arbitrarily small. This model is also

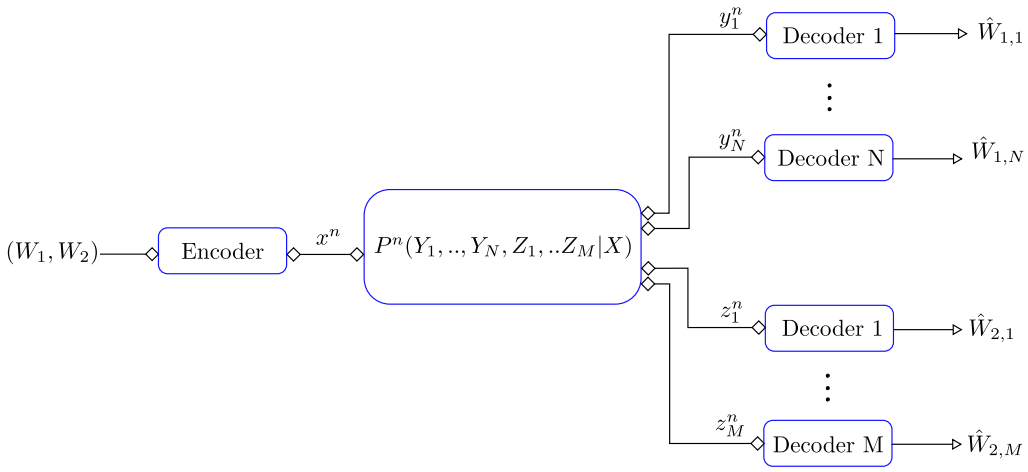


Figure 2: The N by M Compound BC / N by M multi-user BC with two common messages.

equivalent to pairing up users from distinct groups, leading to a compound setting whose class of channels consists of all possible BCs created with possible pairs of users, and where the source is oblivious to the actual channel realization.

2.1 Definition of the Compound Broadcast Channel

- Consider a collection of n-th extensions of discrete memoryless BCs:

$$\{\mathcal{W}_j^n\}_{j\in\mathcal{J}} = \left\{P_{Y_j^n Z_j^n|X^n} : \mathcal{X}^n \longmapsto \mathcal{Y}^n \times \mathcal{Z}^n\right\}, \tag{1}$$

  defined by the conditional pmfs:

$$P_{Y_j^n Z_j^n|X^n} = \prod_{i=1}^{n} P_{Y_{j,i} Z_{j,i}|X_i} \ . \tag{2}$$

- Users' pair of index j takes values in the finite set of indices $\mathcal{J} = [1 : N \times M]$.
- An (M_{1n}, M_{2n}, n)-code for this channel consists of: two sets of messages $\mathcal{M}_1$ and $\mathcal{M}_2$, an encoding function that assigns an n-sequence $x^n(w_1, w_2)$ to each pair of messages $(w_1, w_2) \in \mathcal{M}_1 \times \mathcal{M}_2$ and decoding functions, one at each receiver, that assign to the received signal an estimate message $\hat{w}_k$ in $\mathcal{M}_k$, for $k \in \{1, 2\}$ or an error.

  The probability of error is given by:

$$P_e^{(n)}(j) \triangleq \mathbb{P}\left(\bigcup_{k\in\{1,2\}} \left\{\hat{W}_{k,j} \neq W_k\right\}\right). \tag{3}$$

- A rate pair (R_1, R_2) is said to be achievable if there exists an (M_{1n}, M_{2n}, n)-code satisfying:

$$\liminf_{n\to\infty} \frac{1}{n} \log_2 M_{kn} \geq R_k \quad \forall\, k = \{1, 2\}\,, \tag{4}$$

$$\limsup_{n\to\infty} \max_{j\in\mathcal{J}} P_e^{(n)}(j) = 0\ . \tag{5}$$

  The capacity region is the set of all achievable rate tuples.

3 Outer Bound of the Capacity of the Compound BC

We derive in this section a simple and intuitive outer bound on the capacity region of the compound BC. This outer bound results from a straightforward extension to the compound setting of the best-known outer bound on the capacity of the BC. It will be useful in the examples we shall study later.

Let the rate region $\mathcal{R}_{\text{NEG}}^{(j)}$ denote the Nair & El Gamal outer bound derived in [28], applied to each pair of users with index "j". For the private message setup, the rate region is given by

$$\mathcal{R}_{\text{NEG}}^{(j)}(p_{QUVX}) : \begin{cases} R_1 \leq I(QU; Y_j)\ , \\ R_2 \leq I(QV; Z_j)\ , \\ R_1 + R_2 \leq I(U; Y_j|QV) + I(QV; Z_j)\ , \\ R_1 + R_2 \leq I(QU; Y_j) + I(V; Z_j|QU)\ . \end{cases} \tag{6}$$

for a specific joint pmf on p_{QUVX}. A simple outer bound on the capacity region of the compound BC is stated in the following theorem.

Theorem 16 (Outer bound)**.** *The capacity region of the two-user Compound BC $\mathcal{C}_{\mathcal{J}}$ verifies:*

$$\mathcal{C}_{\mathcal{J}} \subseteq \bigcup_{P_U P_V} \bigcap_{j=1}^{N\times M} \left(\bigcup_{P_{QX|UV}} \mathcal{R}_{NEG}^{(j)}(p_{QUVX})\right)\ , \tag{7}$$

where the channel input X is a deterministic mapping of $\mathcal{Q} \times \mathcal{U} \times \mathcal{V}$.

When the compound BC consists in only one channel, standard non-compound setting, Nair & El Gamal outer bound was not proved to be tight in general. In the relevant compound setting, the fact of optimizing the common auxiliary rv Q for each channel with index j, prevents even more this outer bound from being achievable in the most general case, since the source is oblivious to the channel realization, it thus can not optimize the code for each instance in the compound setting. However, this bound can be tight in some cases as will be clarified later on.

Proof: A sketch of the proof is relegated to Appendix B.3. ■

Chapter 1

Interference Decoding for the Compound BC

In this part of the thesis, we explore a new coding strategy for the Compound BC that relies on Marton's random coding on the encoding side, and the idea of decoding or not the interference at each of the decoders. We denote the combination of these two schemes as Interference Decoding. Our aim is to characterize the gain brought by the involved decoding method and thus, we compare ourselves to the naive scheme where no destination decodes the interfering message, which we name as Non Interference Decoding (NID). We show that for a class of relevant 2 by 1 Compound BCs, the gain of ID over NID is strict, and we even more show that ID is capacity-achieving.

1.1 Interference Decoding for the Compound BC

The inner bound we derive is based on two strategies. The encoding strategy consists in Marton's random coding argument where three codewords, a common codeword and two private codewords encoding each one a message, are generated and mapped via Superposition Coding and Random Binning. The decoding strategy was introduced in the work of Bacelli and El Gamal [14], where roughly speaking, each receiver is allowed to decode its intended message as well as (or not) non-uniquely ([42]) decode the interfering message. Combining this decoding strategy with Marton's random coding arguments is referred to in the sequel as Interference Decoding.

1.1.1 Interference Decoding (ID) Inner Bound

The inner bound we derive here shares common ideas with following works [13]. First, the notion of ID used in [14] where –roughly speaking– each receiver is allowed to decode its intended message as well as (non-uniquely) decode or not the interfering message. Second, the fact that decoding "non-uniquely" the interfering message alleviates an extra constraint on the information rates yielding the same result as if the decoder would have to successively decode the interfering and the intended messages which is related to [42].

Theorem 17 (ID inner bound)**.** *An inner bound on the capacity region of the Compound BC consists in the set of all rates* (R_0, R_1, R_2) *included in:*

$$\mathcal{R}_{ID} \triangleq \bigcup_{p_{QUVX}\in\mathcal{P}} \underbrace{\bigcup_{(T_1,T_2)\in\mathbb{T}(p)}}_{FME} \underbrace{\bigcap_{j=1}^{N\times M}}_{(compound)} \underbrace{\bigcup_{i_j=1}^{4}}_{(4\ methods)} \mathcal{T}_{i_j}^{(j)}(p,T_1,T_2)\ , \tag{1.1}$$

where $\mathcal{P}$ *is the set of all input pmfs* p_{QUVX} *such that* $(Q,U,V) \multimap X \multimap (Y_1,\ldots,Y_N,Z_1,\ldots,Z_N)$*. The rate regions* $\mathcal{T}_{[1:4]}^{(j)}$ *and the set* $\mathbb{T}$ *are, respectively, defined as follows:*

$$\mathcal{T}_1^{(j)}(p,T_1,T_2): \begin{cases} T_1 \leq I(U;Y_j|Q)\ , \\ R_0+T_1 \leq I(QU;Y_j)\ , \\ T_2 \leq I(V;Z_j|Q)\ , \\ R_0+T_2 \leq I(QV;Z_j)\ , \end{cases} \tag{1.2}$$

$$\mathcal{T}_2^{(j)}(p,T_1,T_2): \begin{cases} T_1 \leq I(U;Y_j|Q)\ , \\ R_0+T_1 \leq I(QU;Y_j)\ , \\ T_2 \leq I(V;Z_jU|Q)\ , \\ T_1+T_2 \leq I(UV;Z_j|Q)+I(U;V|Q)\ , \\ R_0+T_1+T_2 \leq I(QUV;Z_j)+I(U;V|Q)\ , \end{cases} \tag{1.3}$$

$$\mathcal{T}_3^{(j)}(p,T_1,T_2): \begin{cases} T_1 \leq I(U;Y_jV|Q)\ , \\ T_1+T_2 \leq I(UV;Y_j|Q)+I(U;V|Q)\ , \\ R_0+T_1+T_2 \leq I(QUV;Y_j)+I(U;V|Q)\ , \\ T_2 \leq I(V;Z_j|Q)\ , \\ R_0+T_2 \leq I(QV;Z_j)\ , \end{cases} \tag{1.4}$$

$$\mathcal{T}_4^{(j)}(p,T_1,T_2): \begin{cases} T_1 \leq I(U;Y_jV|Q)\ , \\ T_1+T_2 \leq I(UV;Y_j|Q)+I(U;V|Q)\ , \\ R_0+T_1+T_2 \leq I(QUV;Y_j)+I(U;V|Q)\ , \\ T_2 \leq I(V;Z_jU|Q)\ , \\ T_1+T_2 \leq I(UV;Z_j|Q)+I(U;V|Q)\ , \\ R_0+T_1+T_2 \leq I(QUV;Z_j)+I(U;V|Q)\ , \end{cases} \tag{1.5}$$

$$\mathbb{T}(p) = \Big\{(T_1,T_2): \quad T_1 \geq R_1\ , \tag{1.6}$$

$$T_2 \geq R_2\ , \tag{1.7}$$

$$T_1+T_2 > R_1+R_2+I(U;V|Q)\Big\}\ . \tag{1.8}$$

Proof: The proof is relegated to Appendix B.1. ■

1.1.2 Discussion on the ID Inner Bound

In the following we give important comments about the ID inner bound and its utility in BCs and Compound BCs.

Remarks 18 (Main comments about the proof)**.** *Each user introduces the union of two sets of constraints, corresponding to decoding or not the interference. This results –in terms of achievable rates– in the union of four rate regions:*

1. *The region $\mathcal{T}_1^{(j)}$ is the same rate region as obtained with Marton's inner bound,*
2. *The region $\mathcal{T}_4^{(j)}$ is obtained by letting the destinations to decode both the intended and the interfering message,*
3. *The regions $\mathcal{T}_2^{(j)}$ and $\mathcal{T}_3^{(j)}$ correspond to each destination decoding the interfering message at once.*

A slightly similar rate region was also derived in [30] in a different context, but it does not take advantage of the encoding technique, and thus in our setting it fails at achieving even Marton's inner bound.

Remarks 19 (Connection to the standard two-user BC)**.** *Consider the standard two-user BC where $\mathcal{J} = 1$. Observe that by allowing both destinations to decode or not the message of the other user –ID scheme– we recover a seemingly larger rate region $\mathcal{R}_{s,ID}$ than that of Marton [3] which does not use the ID technique. Indeed, these regions are given by*

$$\mathcal{R}_{s,ID} \triangleq \bigcup_{p_{QUVX}\in\mathcal{P}} \bigcup_{(T_1,T_2)\in\mathbb{T}(p)} \left(\bigcup_{i=1}^{4} \mathcal{T}_i(p,T_1,T_2) \right) , \tag{1.9}$$

$$\mathcal{R}_{s,NID} \triangleq \bigcup_{p_{QUVX}\in\mathcal{P}} \bigcup_{(T_1,T_2)\in\mathbb{T}(p)} \mathcal{T}_1(p,T_1,T_2) . \tag{1.10}$$

It is clear that $\mathcal{R}_{s,NID} \subseteq \mathcal{R}_{s,ID}$, but the question is whether or not this inclusion is strict. To check this issue, we need to evaluate both regions and thus we resort to FME for (T_1, T_2), and bit recombination between the private rates (R_1, R_2) and the common one R_0[2]. Since the unions commute, we can write that:

$$\begin{aligned} \mathcal{R}_{s,ID} &= \bigcup_{i=1}^{4} \mathcal{R}_{s,i} \\ &= \mathcal{R}_{s,NID} \cup \left(\bigcup_{i=2}^{4} \mathcal{R}_{s,i} \right) , \end{aligned} \tag{1.11}$$

where $\mathcal{R}_{[2:3]}$ are respectively defined by the following sets of inequalities:

$$\mathcal{R}_{s,2} : \left\{ \begin{array}{rcl} R_0 + R_1 & \leq & I(QU;Y) , \\ R_0 + R_1 + R_2 & \leq & I(V;Z|UQ) + I(QU;Y) , \\ R_0 + R_1 + R_2 & \leq & I(QUV;Z) , \end{array} \right. \tag{1.12}$$

$$\mathcal{R}_{s,3} : \left\{ \begin{array}{rcl} R_0 + R_2 & \leq & I(QV;Z) , \\ R_0 + R_1 + R_2 & \leq & I(U;Y|VQ) + I(QV;Z) , \\ R_0 + R_1 + R_2 & \leq & I(QUV;Y) , \end{array} \right. \tag{1.13}$$

[2]For the interested reader a similar calculation is done in Appendix B.4.

$$\mathcal{R}_{s,4}: \begin{cases} R_0+R_1+R_2 & \leq & I(QUV;Y)\ , \\ R_0+R_1+R_2 & \leq & I(QUV;Z)\ , \end{cases} \tag{1.14}$$

while $\mathcal{R}_{s,NID}$ is defined by

$$\mathcal{R}_{s,NID}=\mathcal{R}_{s,1}: \begin{cases} R_0+R_1 & \leq & I(QU;Y)\ , \\ R_0+R_2 & \leq & I(QV;Z)\ , \\ R_0+R_1+R_2 & \leq & I(U;Y|Q)+I(QV;Z)-I(U;V|Q)\ , \\ R_0+R_1+R_2 & \leq & I(QU;Y)+I(V;Z|Q)-I(U;V|Q)\ , \\ 2R_0+R_1+R_2 & \leq & I(QU;Y)+I(QV;Z)-I(U;V|Q)\ . \end{cases} \tag{1.15}$$

From the above rate regions, we observe that by taking $U=Q$, the region $\mathcal{R}_{s,NID}$ contains $\mathcal{R}_{s,2}$, and similarly, setting $V=Q$ allows $\mathcal{R}_{s,NID}$ to contain $\mathcal{R}_{s,3}$ while $U=Q=V$ allows it to contain $\mathcal{R}_{s,4}$. Hence, using the ID strategy in presence of a single channel per user yields the same rate region as Marton's inner bound. Indeed, the apparently gain provided by choosing to decode or not the interference is recovered by an optimization of the input distribution.

We can observe that by resorting to ID in the compound setting, we get a seemingly larger region than Marton's worst-case inner bound, which is given by:

$$\mathcal{R}_{\text{NID}} \triangleq \bigcup_{p_{QUVX}\in\mathcal{P}} \bigcup_{(T_1,T_2)\in\mathbb{T}(p)} \left(\bigcap_{j=1}^{N\times M} \mathcal{T}_1^{(j)}(p,T_1,T_2) \right) . \tag{1.16}$$

It is clear that $\mathcal{R}_{\text{NID}} \subseteq \mathcal{R}_{\text{ID}}$ but yet, no evidence on the strict inclusion has been stated here. In the sequel, we investigate a Compound BC for which the region based on the usual decoding in Marton's inner bound $\mathcal{R}_{\text{NID}}$ fails at achieving the capacity while $\mathcal{R}_{\text{ID}}$ from Theorem 17 is tight. The key point in this "strict inclusion", is that, if the optimizing input pmf varies from one channel to the other (e.g. in terms of superposition ordering of auxiliary RVs), then the joint optimization in the compound setup imposes a stringent limitation on the input pmf. This prevents $\mathcal{R}_{\text{NID}}$ from reaching capacity for some compound models while the ID technique, allowing the choice between two decoding strategies, does not suffer such a loss.

1.2 Interference Decoding is Optimal for a Class of Compound BCs

In this section, we will construct a Compound BC model for which Marton's worst-case inner bound, obtained through NID, is strictly sub-optimal compared to ID inner bound where users are allowed to decode or not the interference. We first discuss a criterion for the construction of such a compound model and later, prove the optimality of ID. For simplicity, we restrict our analysis to the case $\|\mathcal{J}\|=2$ and private rates only, i.e., $R_0=0$.

1.2.1 Irrelevant compound models

The difficulty to characterize optimal coding for the Compound BC is inherent to the class of BCs in the set, i.e., the set of channel users over which we define the compound model. We shall refer to as "irrelevant" models those of ordered BCs for which Marton's worst-case inner bound is tight. As a matter of fact, Marton's inner bound achieves the capacity of every BC for which capacity is known.

Consider the class of broadcast channels:

$$\mathcal{W} = \{\mathcal{W}_1, \mathcal{W}_2\} = \{\mathcal{X} \mapsto (\mathcal{Y}_j, \mathcal{Z}_j)\}_{j\in\{1,2\}} \ , \tag{1.17}$$

where $Y_2 \preccurlyeq Y_1$ and $Z_1 \preccurlyeq Z_2$. Then, it follows that, whatever the auxiliary RVs $(Q, U) \sim p_{QU}$:

$$I(QU; Y_2) \le I(QU; Y_1) \quad , \quad I(U; Y_2|Q) \le I(U; Y_1|Q) \ . \tag{1.18}$$

Thus, Marton's inner bound based on superposition coding and random binning yields the region

$$\begin{cases} R_1 & \le & \min\limits_{j=1,2} I(QU; Y_j) \ , \\ R_2 & \le & \min\limits_{j=1,2} I(QV; Z_j) \ , \\ R_1 + R_2 & \le & \min\limits_{j=1,2} I(U; Y_j|Q) + \min\limits_{j=1,2} I(QV; Z_j) - I(U; V|Q) \ , \\ R_1 + R_2 & \le & \min\limits_{j=1,2} I(QU; Y_j) + \min\limits_{j=1,2} I(V; Z_j|Q) - I(U; V|Q) \ , \end{cases} \tag{1.19}$$

which reduces to:

$$\begin{cases} R_1 & \le & I(QU; Y_2) \ , \\ R_2 & \le & I(QV; Z_1) \ , \\ R_1 + R_2 & \le & I(U; Y_2|Q) + I(QV; Z_1) - I(U; V|Q) \ , \\ R_1 + R_2 & \le & I(QU; Y_2) + I(V; Z_1|Q) - I(U; V|Q) \, . \end{cases} \tag{1.20}$$

This is the the rate region obtained by coding for only the pair of users corresponding to the channel (Y_2, Z_1). Furthermore, it is straightforward to check that if the capacity of this channel is known (e.g. when Y_2 and Z_1 are ordered in the sense of "degradedness" or "less-noisiness"), then Marton's inner bound achieves the capacity region of the Compound BC. Thus, if the marginals seen in set of users 1, i.e., (Y_1, Y_2) are ordered at least in the known senses of "less noisiness", and so are those in the set of users 2, i.e., (Z_1, Z_2), Marton's inner bound for this setup leads to the capacity region of the "worst" BC formed by the worst pair of users in the set. Hence this class of compound models is irrelevant for our purpose.

1.2.2 Compound Binary Erasure and Binary Symmetric BC

In this section, we construct the simplest while relevant Compound BC setting, where:

- Set of user 2 contains only one channel instance, i.e., $Z_1 = Z_2 = Z$.
- Set of user 1 is compound of two possible channel instances denoted by $\{Y_j\}_{j\in\{1,2\}}$.

Table 1.1: Different Orderings allowed by the BEC(e)/BSC(p) BC.

$0 \leq e \leq 2p$	$2p < e \leq 4p(1-p)$	$4p(1-p) < e \leq H_2(p)$	$H_2(p) < e \leq 1$
BSC degraded of BEC	BEC Less Noisy BSC	BEC More Capable BSC	BSC Ess. Less Noisy BEC

Our aim is to show the desired "strict" inclusion $\mathcal{R}_{\text{NID}} \subset \mathcal{R}_{\text{ID}}$. To this end, we need to find a "relevant" compound BC where (Y_1, Y_2) are not strongly ordered (e.g. neither degraded nor less-noisy). Otherwise the resulting Compound BC would be formed by Z and the worst channel between (Y_1, Y_2), for which it is straightforward to see that $\mathcal{R}_{\text{NID}}$ achieves the capacity region.

Besides this argument, if we are to show the strict inclusion of Marton's rate region with respect to the rate region obtained by ID, we need to provide for some inverse orderings in the compound channels formed by all possible pairs of users, so as to impose a tradeoff between two antagonist coding schemes for Marton's coding scheme, i.e., two antagonist choices of auxiliary RVs at the encoder. One can then think of a setting where for instance the BC (Y_1, Z) has Z "better" than Y_1 while the BC (Y_2, Z) is ordered in the opposite way, i.e Y_2 is better than Z.

Consider the *Binary Erasure Channel* (BEC) with erasure probability e and the *Binary Symmetric Channel* (BSC) with crossover probability p. These have the particularity of allowing for a variety of orderings between the outputs [29], depending on (e, p), as summarized in Table 1.1. Define the Compound BC with components:

$$\mathcal{W} : \begin{cases} \mathcal{X} & \longmapsto & \mathcal{Z} \equiv \text{BSC(p)}\,, \\ \mathcal{X} & \longmapsto & \mathcal{Y}_1 \equiv \text{BSC}(p_1)\,, \\ \mathcal{X} & \longmapsto & \mathcal{Y}_2 \equiv \text{BEC}(e_2)\,. \end{cases} \tag{1.21}$$

We first start by imposing to Y_2 to be more capable than Y_1, which requires: $4p_1(1-p_1) < e_2 \leq H_2(p_1)$. One possible choice is then to take Y_1 as a *physically degraded* version of Z, i.e., $p < p_1 < 0.5$, and Y_2 more capable than Z, i.e.,

$$4p(1-p) < 4p_1(1-p_1) < e_2 \leq H_2(p) \leq H_2(p_1)\ . \tag{1.22}$$

This choice fulfils the criteria stated for the construction of a relevant example. For this case, the simple outer bound enunciated in Section 3 writes as:

$$\mathcal{C}_{\mathcal{J}} \subset \mathcal{C}_1 \cap \mathcal{C}_2\ , \tag{1.23}$$

where:

$$\mathcal{C}_1 : \begin{cases} R_1 & \leq & 1 - H_2(p_1 \star \alpha)\ , \\ R_2 & \leq & H_2(p \star \alpha) - H_2(p)\ , \end{cases} \tag{1.24}$$

$$\mathcal{C}_2 : \begin{cases} R_1 & \leq & (1-e_2)\, H_2(\alpha)\ , \\ R_2 & \leq & 1 - H_2(p \star \alpha)\ , \\ R_1 + R_2 & \leq & (1-e_2)\ . \end{cases} \tag{1.25}$$

We claim that the capacity region $\mathcal{C}_1$ is strictly included in $\mathcal{C}_2$, for which we can compare:

$$\max_{(R_1,R_2)\in\mathcal{C}_1} \frac{R_1}{(1-H_2(p))-R_2} = \lim_{\alpha\to 1/2} \frac{1-H_2(p_1\star\alpha)}{1-H_2(p\star\alpha)} \approx \frac{(1-2p_1)^2}{(1-2p)^2} \tag{1.26}$$

and

$$\max_{(R_1,R_2)\in\mathcal{C}_2} \frac{R_1}{(1-H_2(p))-R_2} \geq \frac{1-e_2}{1-H_2(p)} \ . \tag{1.27}$$

Our claim simply follows by noticing that from the assumptions on the parameters e_2, p and p_1, we have that:

$$\frac{(1-2p_1)^2}{(1-2p)^2} \leq 1 \leq \frac{1-e_2}{1-H_2(p)} \ , \tag{1.28}$$

which shows the outer bound reduces to $\mathcal{C}_1$.

1.2.3 Evaluation of the ID inner bound of Theorem 17

We evaluate the proposed rate region $\mathcal{R}_{\text{ID}}$ of Theorem 17, which satisfies:

$$\mathcal{R}_{\text{ID}} \supseteq \bigcup_{p_{QUVX}\in\mathcal{P}} \bigcup_{(T_1,T_2)\in\mathbb{T}(p)} \left(\mathcal{T}_3^{(1)}(p,T_1,T_2)\cap\mathcal{T}_4^{(2)}(p,T_1,T_2)\right) \ , \tag{1.29}$$

where $\mathcal{T}_3^{(1)}\cap\mathcal{T}_4^{(2)}$ is defined by the set of inequalities:

$$\begin{cases} T_2 \leq I(V;ZU|Q) \ , \\ T_1+T_2 \leq I(UV;Z|Q)+I(U;V|Q) \ , \\ R_0+T_1+T_2 \leq I(QUV;Z)+I(U;V|Q) \ , \\ T_1 \leq I(U;Y_2V|Q) \ , \\ T_1+T_2 \leq I(UV;Y_2|Q)+I(U;V|Q) \ , \\ R_0+T_1+T_2 \leq I(QUV;Y_2)+I(U;V|Q) \ , \\ T_1 \leq I(U;Y_1|Q) \ , \\ R_0+T_1 \leq I(QY;Y_1) \\ T_1\geq R_1 \quad , \quad T_2\geq R_2 \ , \\ T_1+T_2 > R_1+R_2+I(U;V|Q) \ . \end{cases} \tag{1.30}$$

This comes to choosing: $i_1=3$, i.e., using decoding method (3) for the BC (1), while the other channel gets the fourth decoding method: $i_2=4$. These constraints allow Z and Y_2 to decode all messages, while forcing Y_1 to decode only its own message. In Appendix B.4, it is shown after FME on (T_1,T_2), bit recombination, and then setting $R_0=0$, that the previous rate region reduces to the set of rates satisfying:

$$\begin{cases} R_1 \leq I(QU;Y_1) \ , \\ R_1+R_2 \leq I(QU;Y_1)+I(V;Z|QU) \ , \\ R_1+R_2 \leq I(QU;Y_1)+I(UV;Y_2|Q) \ , \\ R_1+R_2 \leq I(QUV;Y_2) \ . \end{cases} \tag{1.31}$$

Then, letting: $V=X$, $\bar{Q}=(Q,U)$, and using the fact that Y_2 is *more capable* than Z, yields:

$$\begin{cases} R_1 \leq I(\bar{Q};Y_1) \ , \\ R_1+R_2 \leq I(\bar{Q};Y_1)+I(X;Z|\bar{Q}) \ . \end{cases} \tag{1.32}$$

This achievable rate region coincides with the outer bound and thus provides the capacity region of the BC (Y_1, Z) for the considered setup. Letting then $\bar{Q} \longmapsto X \equiv \text{BSC}(\alpha)$, and $X \sim \text{Bern}(1/2)$ we get the following union over all $\alpha \in [0:1]$ of:

$$\mathcal{R}_{\text{ID}} : \left\{ \begin{array}{rcl} R_1 & \leq & 1 - H_2(p_1 \star \alpha) \ , \\ R_1 + R_2 & \leq & 1 - H_2(p_1 \star \alpha) + H_2(p \star \alpha) - H_2(p) \ . \end{array} \right. \tag{1.33}$$

In order to check that $\mathcal{R}_{\text{ID}}$ is equal to the outer bound $\mathcal{C}_1$, we should first start by noticing that it is the exclusive union of two rate regions: $\mathcal{C}_1$ and $\mathcal{R}_E$ which are defined by

$$\mathcal{R}_E : \left\{ \begin{array}{rcl} R_2 & \geq & H_2(p \star \alpha) - H_2(p) \ , \\ R_1 + R_2 & \leq & 1 - H_2(p_1 \star \alpha) + H_2(p \star \alpha) - H_2(p) \ . \end{array} \right. \tag{1.34}$$

As plot in Fig. 1.1, this region has four corner points among which three are clearly included in $\mathcal{C}_1$, i.e., A, B, and C.

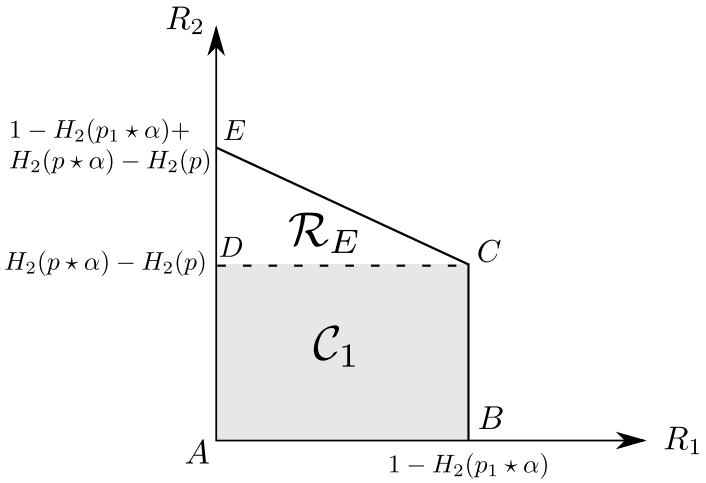


Figure 1.1: Comparison between $\mathcal{C}_1$ and $\mathcal{R}_{\text{ID}}$.

To show that the point E lies in the region $\mathcal{C}_1$, we first write that:

$$E = (0, 1 - H_2(p_1 \star \alpha) + H_2(p \star \alpha) - H_2(p)) \ . \tag{1.35}$$

Since Y_1 is physically degraded with respect to Z, i.e., $p \leq p_1$, and since α, $p \star \alpha$ and $p_1 \star \alpha$ are all included in the interval $[0 : 0.5]$, one can clearly write that: $-H_2(p_1 \star \alpha) + H_2(p \star \alpha) \leq 0$. Hence, the point E is dominated by the point $C_2 = (0; 1 - H_2(p))$, which is already achievable in $\mathcal{C}_1$. The line between C and E can is achieved by the convexity of the rate region $\mathcal{C}_1$.

1.2.4 Outer bound on Marton's inner bound

When restricted to Marton's inner bound, the rate region in expression (1.16) is included in the union of next constraints:

$$\left\{\begin{array}{rcl} T_2 & \leq & I(V;Z|Q)\ , \\ R_0+T_2 & \leq & I(QV;Z)\ , \\ T_1 & \leq & \min\limits_{j=1,2} I(U;Y_j|Q)\ , \\ R_0+T_1 & \leq & \min\limits_{j=1,2} I(QU;Y_j)\ , \\ T_1\geq R_1 & , & T_2\geq R_2\ , \\ T_1+T_2 & > & R_1+R_2+I(U;V|Q)\ . \end{array}\right. \tag{1.36}$$

Then, we perform FME on the rates T_1 and T_2, bit recombination, and we set $R_0=0$, which yields the following rate region:

$$\left\{\begin{array}{rcl} R_2 & \leq & I(QV;Z) \\ R_1 & \leq & \min\limits_{j=1,2} I(QU;Y_j)\ , \\ R_1+R_2 & \leq & I(V;Z|Q)+\min\limits_{j=1,2} I(QU;Y_j)-I(U;V|Q)\ , \\ R_1+R_2 & \leq & I(QV;Z)+I(U;Y_2|Q)-I(U;V|Q)\ , \end{array}\right. \tag{1.37}$$

where we have used the fact that: $I(Q;Y_1)\leq I(Q;Z)$, i.e., *physical degradedness*. As a matter of fact, the previous rate region is contained in the set of rates verifying:

$$\left\{\begin{array}{rcl} R_1 & \leq & \min\limits_{j=1,2} I(QU;Y_j)\ , \\ R_1+R_2 & \leq & I(X;Z|QU)+\min\limits_{j=1,2} I(QU;Y_j)\ , \end{array}\right. \tag{1.38}$$

because for each $P_{QUVX}\in\mathcal{P}$ the next inequalities hold:

$$I(QV;Z)\leq I(X;Z)\,, \tag{1.39}$$

$$I(V;Z|Q)+\min_{j=1,2} I(QU;Y_j)-I(U;V|Q)\leq I(X;Z|QU)+\min_{j=1,2} I(QU;Y_j) \tag{1.40}$$

$$\leq I(X;Z)\ . \tag{1.41}$$

By letting $\bar{Q}=(Q,U)$, we obtain the following constraints:

$$\mathcal{R}_{\text{OuterNID}}:\left\{\begin{array}{rcl} R_1 & \leq & \min\limits_{j=1,2} I(\bar{Q};Y_j)\ , \\ R_1+R_2 & \leq & I(X;Z|\bar{Q})+\min\limits_{j=1,2} I(\bar{Q};Y_j)\ . \end{array}\right. \tag{1.42}$$

In Appendix B.5, we show that it suffices to evaluate this bound for all auxiliary RVs $\bar{Q}$ that verify $\|\bar{Q}\|\leq 4$ and $X\sim\text{Bern}(1/2)$.

Though we might state such characteristics about the maximizing distribution, the optimization of this region turns out to be tricky since the usual bounding tools such as "Mrs. Gerber's Lemma" leads only to the next lower bound:

$$\mathcal{R}_{\text{Lower,NID}}\subseteq\left\{\begin{array}{rl} R_2 & \leq H_2(p\star\alpha)-H_2(p)\ , \\ R_1 & \leq \min\{1-H_2(p_1\star\alpha),\bar{e}_2(1-H_2(\alpha))\}\ . \end{array}\right. \tag{1.43}$$

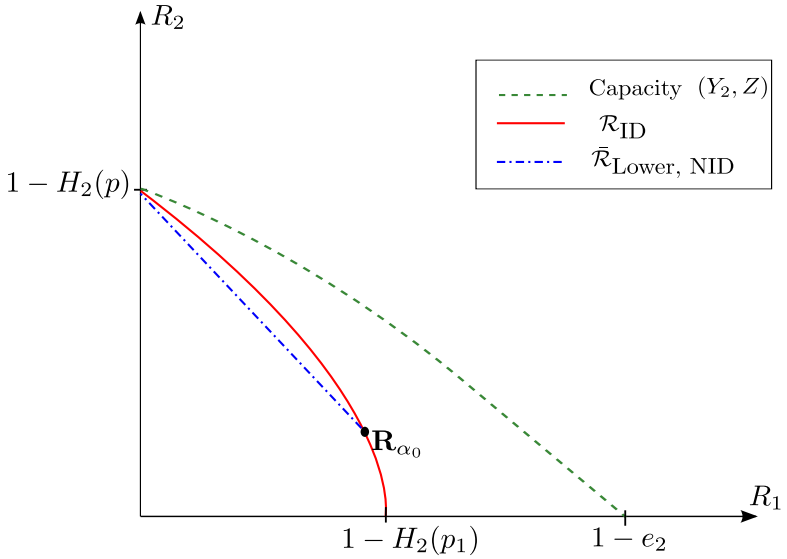


Figure 1.2: Comparison between the rate region $\mathcal{R}_{\text{ID}}$ and the convex closure or $\mathcal{R}_{\text{Lower,NID}}$.

Fig. 1.2 plots a comparison between these two regions. This lower bound coincides with the capacity region $\mathcal{R}_{\text{ID}}$ over the interval $R_2 \in [0 : H_2(p \star \alpha_0) - H_2(p)]$ or equivalently $R_1 \in [0 : 1 - H_2(p_1 \star \alpha_0)]$ where α_0 is given by: $1 - H_2(p_1 \star \alpha_0) = (1 - e_2)(1 - H_2(\alpha_0))$.

In order to derive an upper bound, we study a looser outer bound to $\mathcal{R}_{\text{Outer,NID}}$, provided that the gap stays strict between the capacity region and this outer bound. Let us define the function $t : [0 : 1 - H_2(p)] \mapsto \Re_+$ as:

$$t(x) \triangleq \sup_{p_{XQ} \in \mathcal{C}(x)} \min\{I(Q;Y_1), I(Q;Y_2)\} \ , \tag{1.44}$$

where the class $\mathcal{C}(x)$ is given by

$$\mathcal{C}(x) = \Big\{ p_{XQ} \in \mathcal{P}(\mathcal{X} \times \mathcal{Q}) : \quad Q \multimap X \multimap (Z, Y_1, Y_2) \\ X \sim \text{Bern}(1/2) \ , \ I(X;Z|Q) \geq x \Big\} \ . \tag{1.45}$$

The function $t : x \mapsto t(x)$ characterizes the convex closure of the region $\bar{\mathcal{R}}_{\text{Outer,NID}}$, i.e., $(R_1, R_2) \in \bar{\mathcal{R}}_{\text{Outer,NID}}$ thus $R_1 = t(R_2)$. In the same way, define t_1 over $[0 : 1 - H_2(p)]$ by

$$t_1(x) \triangleq \sup_{p_{XQ} \in \mathcal{C}(x)} I(Q;Y_1) \ , \tag{1.46}$$

where t_1 characterizes the convex closure of the region $\bar{\mathcal{R}}_{\text{ID}}$.

In the sequel, we work towards a closed form evaluation of an upper bound of t that would still be dominated by t_1.

1.2.5 An upper bound on the function $t(x)$

We follow the method in [43] where

$$t(x) \triangleq \sup_{p_{XQ} \in \mathcal{C}(x)} \min\left\{I(Q;Y_1) \, , \, I(Q;Y_2)\right\} \tag{1.47}$$

$$= \sup_{p_{XQ}\in\mathcal{C}(x)} \min_{a\in[0:1]} \Big[a\, I(Q;Y_1) + \bar{a}\, I(Q;Y_2)\Big] \tag{1.48}$$

$$\leq \min_{a\in[0:1]} \sup_{p_{XQ}\in\mathcal{C}(x)} \Big[a\, I(Q;Y_1) + \bar{a}\, I(Q;Y_2)\Big] \ , \tag{1.49}$$

for all $x \in [0 : 1 - H_2(p)]$. Let define for each $a \in [0 : 1]$ and $t_a \in [0 : 1 - H_2(p)]$,

$$t_a(x) \triangleq \sup_{p_{XQ}\in\mathcal{C}(x)} \Big[a\, I(Q;Y_1) + \bar{a}\, I(Q;Y_2)\Big] \ . \tag{1.50}$$

Notice that:

- The case $a = 1$ was already studied in [43] and it was shown that:

$$t_1(x) = 1 - H_2(p_1 \star p_x) \ , \tag{1.51}$$

  where $H_2(p \star p_x) - H_2(p) = x$.

- The case $a = 0$ can be studied in a very similar fashion as in [43] by finding out that:

$$t_0(x) = \inf_{\lambda\in\mathcal{R}^+} [F_0(\lambda) - \lambda\, x] \tag{1.52}$$

$$= (1 - e_2) \left(1 - \frac{x}{1 - H_2(p)}\right) \ , \tag{1.53}$$

  where:

$$F_0(\lambda) = \max\left\{(1 - H_2(p))\, \lambda, (1 - e_2)\right\} \ . \tag{1.54}$$

Now, to upper bound t_a, we could have written that:

$$t_a(x) \leq a \sup_{\mathcal{C}(x)} I(Q;Y_1) + \bar{a} \sup_{\mathcal{C}(x)} I(Q;Y_2) \tag{1.55}$$

$$= a\, t_1(x) + \bar{a}\, t_0(x) \tag{1.56}$$

$$\geq t_1(x) \ , \tag{1.57}$$

where (1.57) follows from what we have proved in Section 1.2.2, i.e., t_0 dominates t_1 over the interval $[0 : 1 - H_2(p)]$. Thus, we cannot restrict ourselves to the upper bound in (1.55) on t_a since it is rather loose, and we will hence bound more tightly the function t_a.

Proposition 4. *The function t_a satisfies the following properties:*

(i) For all $x \in [0 : 1 - H_2(p)]$,

$$t_a(x) = \max_{p_{XQ}\in\mathcal{C}(x)} [a\, I(Q;Y_1) + \bar{a}\, I(Q;Y_2)] \ , \tag{1.58}$$

(ii) t_a is concave in x,

(iii) t_a can be described identically by its supporting lines,

(iv) t_a is decreasing in x.

Proof: The proof is relegated to Appendix B.6. ■

The next result is rather crucial since it allows us to transform the optimization of a rate region into optimizing one quantity captured in $F_a(\lambda)$.

Corollary The following conclusions can be drawn:

(a) The constraint in (1.45) can be transformed into:

$$I(X;Z|Q) = x \ . \tag{1.59}$$

(b) We have that:

$$t_a(x) = \inf_{\lambda \in \mathcal{R}^+} \left[\max_{\mathcal{P}(\mathcal{X}\times\mathcal{Q})} \Big[a\, I(Q;Y_1) + \bar{a}\, I(Q;Y_2) + \lambda\, I(X;Z|Q) \Big] - \lambda\, x \right] \tag{1.60}$$

$$= \inf_{\lambda \in \mathcal{R}^+} \Big[F_a(\lambda) - \lambda\, x \Big] \ , \tag{1.61}$$

where

$$F_a(\lambda) \triangleq \max_{p_{XQ} \in \mathcal{P}(\mathcal{X}\times\mathcal{Q})} \Big[a\, I(Q;Y_1) + \bar{a}\, I(Q;Y_2) \Big] \ . \tag{1.62}$$

Proof: (a) follows from the non-increasing property of t_a and (b) follows from the concavity of the function t_a since a concave function can be described by its supporting lines [44]. ■

The analysis of the function t_a for an arbitrary a brings about significant computational complexity, we thus only chose to plot it using stochastic optimization methods. We chose $e_2 = 0.46$, $p = 0.1$ and $p_1 = 0.13$. It can be readily shown that these parameters verify (1.22).

In Fig. 1.3, we chose $a = 0.92$ and plot the normalized difference function:

$$d_a(R_1) = \frac{t_1^{-1}(R_1) - t_a^{-1}(R_1)}{\max(\mid t_1^{-1}(R_1) - t_a^{-1}(R_1) \mid)} \ , \tag{1.63}$$

over the interval of interest: $[0 : 1 - H_2(p_1 \star \alpha_0)]$ where: $1 - H_2(p_1 \star \alpha_0) = (1 - e_2)(1 - H_2(\alpha_0))$. The function d_a being strictly positive, the claim of strict inclusion is thus shown.

We have investigated so far the role that alternative decoding techniques, namely "Interference Decoding", play in the Compound BC where the users present a given hierarchy unknown at the encoder. The decoding technique takes advantage of the many possible decoding ways to alleviate the constraint of superposition coding at the source which allows the latter to apply a "symmetric" encoding rule regardless of which channel controls the communication. In the sequel, we analyse a class of non-ordered Compound BC to infer novel strategies when there is no specific order between channels users. In this case, we will not seek to optimize the decoder but rather the encoding technique.

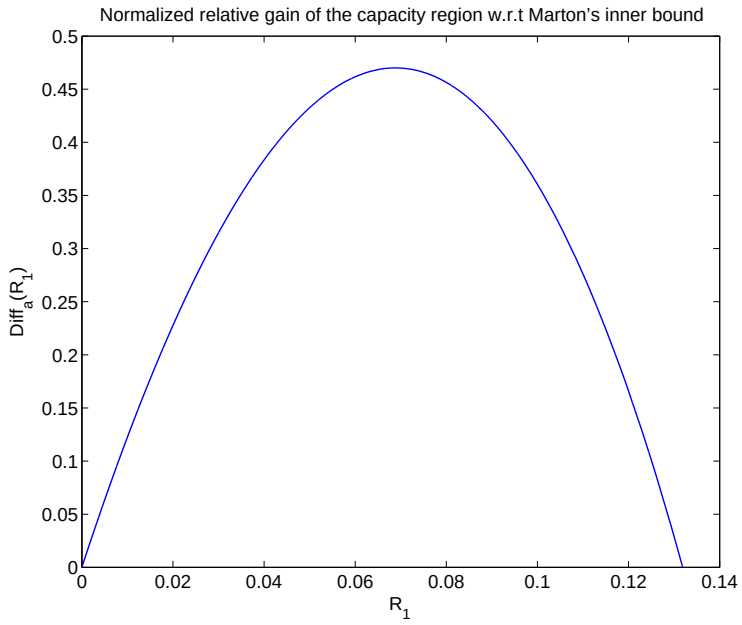


Figure 1.3: $d_a(R_1)$ the normalized relative gain of the capacity region with respect to Marton's inner bound for $a = 0.92$, $e_2 = 0.46$, $p = 0.1$ and $p_1 = 0.13$.

Chapter 2

Multiple Description Coding for the Compound BC

In this part of the work, we investigate another coding strategy that can enhance the achievable rates in a compound setting: Multiple Description coding. The utility of this scheme arises especially when no sort of order between the many possible instances of the same user exists.

2.1 Multiple Description Coding in the Compound BC

In this section, we investigate a coding technique, referred to as "Multiple Description (MD) coding", that can enhance the achievable rates in the Compound BC. The utility of this coding arises especially when no sort of order between the many possible instances of the users channels exists. The main idea behind MD coding is to convey the message intended to the many instances of the same group of users, through a common description as well as a set of dedicated private descriptions which can be easily decoded each at their respective instances. The common description –to be decoded by all users– will suffer from the compound setup in that the rate has to be small enough to be decodable by all users in the same group whereas the private descriptions suffer no such loss. It is worth mentioning here that the introduction of private descriptions will also result in a loss tantamount to their "correlation cost". We aim at exploring the utility of MD coding in the Compound BC setting.

In the sequel, for a matter of conciseness, we choose to address the Compound BC setting when only one user has two possible channels, namely Y_1 or Y_2, whilst the other user suffers from no such uncertainty Z. We first derive two inner bounds on the capacity region to be compared: the Common Description (CD) inner bound that is equivalent to Marton's worst-case inner bound, and the MD inner bound. We then specialize the bounds to the Compound MISO BC and show how MD coding outperforms the standard CD coding. Finally, we analyze the behavior of the obtained rate regions compared to our outer bound.

2.1.1 Multiple Description (MD) Inner Bound

Theorem 20 (MD inner bound)**.** *An inner bound on the capacity region of* 2×1 *Compound BC is given by the set of rate pairs* (R_1, R_2) *satisfying:*

$$R_1 \leq I(U_0U_1; Y_1|Q) \ , \tag{2.1a}$$
$$R_1 \leq I(U_0U_2; Y_2|Q) \ , \tag{2.1b}$$
$$2R_1 \leq I(U_0U_1; Y_1|Q) + I(U_0U_2; Y_2|Q) - I(U_1; U_2|QU_0) \ , \tag{2.1c}$$
$$R_2 \leq I(V; Z|Q) \ , \tag{2.1d}$$
$$R_1 + R_2 \leq I(U_0U_1; Y_1|Q) + I(V; Z|Q) - I(U_0U_1; V|Q) \ , \tag{2.1e}$$
$$R_1 + R_2 \leq I(U_0U_1; Y_2|Q) + I(V; Z|Q) - I(U_0U_2; V|Q) \ , \tag{2.1f}$$
$$2R_1 + R_2 \leq I(U_0U_1; Y_1|Q) + I(U_0U_2; Y_2|Q) + I(V; Z|Q) - I(U_0U_1U_2; V|Q) - I(U_1; U_2|QU_0) \ , \tag{2.1g}$$
$$2R_1 + 2\,R_2 \leq I(U_0U_1; Y_1|Q) + I(U_0U_2; Y_2|Q) + 2I(V; Z|Q) - I(U_0U_1; V|Q) - I(U_0U_2; V|Q) - I(U_1; U_2|QU_0V) \ , \tag{2.1h}$$

for some set of arbitrarily correlated RVs of joint pmf: $P_{QU_0U_1U_2VX}$ *such that the Markov chain* $(Q, U_0, U_1, U_2, V) \multimap X \multimap (Y_1, Y_2, Z)$ *holds.*

Proof: The proof is given in Appendix C.1. ■

2.1.2 Common Description (CD) Inner Bound

Inspired by Marton's inner bound, we can derive what we call the "common description" (CD) coding –worst-case of Marton's inner bound– that consists of all rate pairs (R_1, R_2) verifying:

$$R_1 \leq \min_{j\in\{1,2\}} I(U; Y_j|Q) \ , \tag{2.2a}$$
$$R_2 \leq I(V; Z|Q) \ , \tag{2.2b}$$
$$R_1 + R_2 \leq \min_{j\in\{1,2\}} I(U; Y_j|Q) + I(V; Z|Q) - I(U; V|Q) \ , \tag{2.2c}$$

where U, V and Q are arbitrarily correlated auxiliary RVs.

Without time-sharing, this inner bound imposes that both users in the compound setting decode the same set of variables and does not allow to treat the two possible outputs differently. However, time-sharing helps enhance the performance of this region since it allows for different signalling strategies across the time slots. The combination of the two techniques is denoted in literature as "symbol or block expansion" [33] and allows CD coding to achieve the optimal DoF for some classes of the compound MISO BC. It is easy to check that MD inner bound (2.1) recovers the CD inner bound (2.2) by setting both private descriptions equal to: $U_1 \equiv \emptyset$ and $U_2 \equiv \emptyset$. Thus, implying that Marton's inner bound can achieve the optimal DoF for the compound 2×1 Gaussian MISO BC, the question of whether MD inner bound can strictly improve on CD inner bound arises, and will be investigated in this section.

2.1.3 MD Coding over the standard BC and the Compound Channel

In this section, we elaborate on the fact that CD coding performs at least as good as MD coding in both the standard BC and the Compound Point-To-Point Channel.

As for the Compound Channel, let us assume that we have a compound model with two possible channel outputs denoted by Y_1 and Y_2. We want to show that, for all joint pmfs $P_{U_0U_1U_2X}$ there exists a common auxiliary RV $U_0^\star$ that yields a rate greater than the one achieved by using MD coding. Let

$$R(P_{U_0U_1U_2X}) \triangleq \min\Big\{I(U_0U_1;Y_1)\,,\, I(U_0U_2;Y_2)\,, \tag{2.3}$$

$$\frac{1}{2}\Big[I(U_0U_1;Y_1)+I(U_0U_2;Y_2)-I(U_1;U_2|U_0)\Big]\Big\}\,, \tag{2.4}$$

where we have that:

$$I(U_0U_1;Y_1) \le I(U_0U_1U_2;Y_1)\,, \tag{2.5}$$

$$I(U_0U_2;Y_2) \le I(U_0U_1U_2;Y_2)\,, \tag{2.6}$$

$$I(U_0U_1;Y_1)+I(U_0U_2;Y_2)-I(U_1;U_2|U_0) \le I(U_0U_1U_2;Y_1)+I(U_0U_1U_2;Y_2)\,, \tag{2.7}$$

and thus,

$$R(P_{U_0U_1U_2X}) \le \min\left\{I(U_0U_1U_2;Y_1)\,,\, I(U_0U_1U_2;Y_2)\right\}\,. \tag{2.8}$$

By letting $U_0^\star = (U_0U_1U_2)$, the desired equality holds[3]:

$$\max_{P_{U_0U_1U_2X}} R(P_{U_0U_1U_2X}) = \max_{P_{U_0X}} \min\{I(U_0;Y_1), I(U_0;Y_2)\}\,. \tag{2.9}$$

Further, for the case of the standard BC it turns out that MD coding do not help much neither. To check this, for $Y_1 \equiv Y_2$, fix a joint pmf $P_{U_0U_1U_2|X}$ and let us assume that

$$I(U_0U_1;Y_1) - I(U_0U_1;V) \le I(U_0U_2;Y_1) - I(U_0U_2;V)\,. \tag{2.10}$$

Then, it is easy to see that the choice $U^\star = (U_0U_2)$ and $U_1^\star = U_2^\star = \emptyset$ allows us to get:

$$R(P_{U_0U_1U_2X}) \le \max_{p_{U_0X}}\{I(U_0;Y_1) - I(U_0;V)\}\,. \tag{2.11}$$

Hence,

$$\max_{P_{U_0U_1U_2X}} R(P_{U_0U_1U_2X}) = \max_{P_{U_0X}} \min\left\{I(U_0;Y_1)\,,\, I(U_0;Y_2)\right\}\,. \tag{2.12}$$

Needless to say that in the compound BC, the previous assertion is not true any longer since it is not known whether the inequalities:

$$I(U_0U_1;Y_1) - I(U_0U_1;V) \le I(U^\star;Y_1) - I(U^\star;V)\,, \tag{2.13}$$

$$I(U_0U_2;Y_2) - I(U_0U_2;V) \le I(U^\star;Y_2) - I(U^\star;V)\,, \tag{2.14}$$

$$\sum_{j=1}^{2}\left[I(U_0U_j;Y_j) - I(U_0U_j;V)\right] - I(U_1;U_2|U_0V) \le \sum_{j=1}^{2}\left[I(U^\star;Y_j) - I(U^\star;V)\right]\,, \tag{2.15}$$

still hold for some $U^\star$, and this is the key reason for which MD is useful. However, MD proves to be useless in the cases of the BC and the Compound Channel while no evidence on its role in the Compound BC was stated. This motivates the following comparison between the CD and MD coding techniques for the 2×1 Compound MISO BC.

[3]The inequality in the inverse order is trivial by setting $U_1 = U_2 = \emptyset$.

2.2 The Real Compound MISO BC and MD Based DPC

The optimal transmit strategy for the non-ordered Gaussian MISO BC is to apply Dirty-Paper Coding [15, 16], which is a non-linear coding technique that allows the decoder to suppress the interference. In the sequel, we derive the inner bounds resulting from an adequate use of the DPC scheme with the MD coding technique, referred to as MD-DPC, and later study a specific class of Compound MISO BC for which MDs are of consequent utility compared to the basic CD coding, referred to as CD-DPC.

Consider the Compound MISO BC which consists of a source equipped with 2 antennas and 2 single antenna receivers. Receiver 1 has two possible outputs, namely, Y_1 and Y_2, and let Z be the channel output of the receiver 2, where these outputs at time $i = [1, \ldots, n]$ are given by

$$\left\{ \begin{array}{rcl} y_{j,i} & = & \mathbf{h}_j^t \, \mathbf{x}_i + n_{j,i} \ , \\ z_i & = & \mathbf{g}^t \, \mathbf{x}_i + w_i \ , \end{array} \right. \tag{2.16}$$

for $j \in \{1, 2\}$, where: $\mathbf{h}_j$ and $\mathbf{g}$ are 2×1 generic real channel vectors that are assumed to be constant throughout the transmission. Moreover, it is assumed that any subset of 2 channels among them are linearly independent; $\mathbf{x}$ is the 2×1 power limited channel input vector so that $\mathbb{E}[\mathbf{x}^t \mathbf{x}] \leq P$ and last, the noise sequences $\{n_{j,i}\}$ and $\{w_i\}$ are assumed to be i.i.d. draws according to a standard Gaussian distribution $\mathcal{N}(0, N)$.

In this section, we will compare the CD to the MD inner bound under two different coding techniques depending on the correlation between the private auxiliary RVs. We first start with the case where the private descriptions are *uncorrelated* in the way that the encoder communicates part of the time a private description U_1 to help user Y_1 to decode the intended message, and a private description U_2 during the remaining part of the time to help user Y_2. Later, we consider *arbitrary correlation* between the private descriptions in that both are transmitted all along time, resulting in a non-zero correlation cost.

2.2.1 Preliminaries and Useful Definitions

In the sequel, we resort to DPC [16] in its vector formulation, thus some basic definitions and analytic formulas will be introduced herein to lighten the notation afterwards.

Let us consider the following coding scheme:

$$\left\{ \begin{array}{rcl} U_0 & = & X_u + \alpha X_v \ , \\ V & = & X_v \ , \\ \mathbf{X} & = & X_u \, \mathbf{B}_u + X_v \, \mathbf{B}_v \ , \end{array} \right. \tag{2.17}$$

where $X_u \sim \mathcal{N}(0, P_u)$ and $X_v \sim \mathcal{N}(0, P_v)$ are independent RVs such that $P_u + P_v \leq P$. It is then easy to check that:

$$I(U_0; Y_j) - I(U_0; V) = \log_2 \left(\frac{h_{j,u}^2 P_u + N}{I_j (\alpha - \beta_j)^2 + N} \right) \ , \tag{2.18}$$

where:

$$\beta_j = \frac{P_u \, h_{j,u} \, h_{j,v}}{h_{j,u}^2 \, P_u + N} \quad \text{and} \quad I_j = \left(\frac{P_v}{P_u} \right) \frac{\left(h_{j,u}^2 P_u + N \right)^2}{h_{j,u}^2 P_u + h_{j,v}^2 P_v + N} \ . \tag{2.19}$$

We now choose to transmit an additive private description $X_p \sim \mathcal{N}(0, x)$ while keeping the total useful power equal to P_u, i.e., $0 \leq x \leq P_u$. Then, with the following coding scheme:

$$\left\{ \begin{array}{rcl} U_0 & = & X_u + \alpha X_v \ , \\ U_j & = & X_p + \alpha_j X_v \ , \\ \mathbf{X} & = & (X_u + X_p)\mathbf{B}_u + X_v \mathbf{B}_v \ , \end{array} \right. \tag{2.20}$$

we can optimize the value of the private DPC parameter α_j to state the following result.

Lemma 1 (Optimizing the private descriptions)**.**

$$\max_{\alpha_j \in \mathbb{R}} \Big[I_{\alpha_j}(U_0 U_j; Y_j) - I_{\alpha_j}(U_0 U_j; V) \Big] = \frac{1}{2} \log_2 \left(\frac{h_{j,u}^2 P_u + N}{\dfrac{I_j^x N (\alpha - \beta_j^x)^2}{h_{j,u}^2 x + N} + N} \right) \ , \tag{2.21}$$

and where, for $j \in \{1, 2\}$, we have:

$$\beta_j^x = \frac{(P_u - x)\, h_{j,u}\, h_{j,v}}{h_{j,u}^2 P_u + N} \quad \textit{and} \quad I_j^x = \left(\frac{P_v}{P_u - x} \right) \frac{\left(h_{j,u}^2 P_u + N \right)^2}{h_{j,u}^2 P_u + h_{j,v}^2 P_v + N} \ . \tag{2.22}$$

Proof: The key point of the proof is that the private description, when optimized, yields an interference free link:

$$\max_{\alpha_j \in \mathbb{R}} \Big[I_{\alpha_j}(U_j; Y_j | U_0) - I_{\alpha_j}(U_j; V | U_0) \Big] = I(X_p; Y_j | X_u X_v) \tag{2.23}$$

$$= \frac{1}{2} \log_2 \left(\frac{h_{j,u}^2 x + N}{N} \right) \ . \tag{2.24}$$

The rest of the proof is relegated to Appendix C.3. ■

2.2.2 Common Description DPC (CD-DPC)

Consider the channel model defined by (2.16) and let us define the two following rate regions resulting from two antagonist DPC schemes:

$$\mathcal{R}_1 : \left\{ \begin{array}{rcl} R_1 & \leq & \max\limits_{\alpha} \min\limits_{j \in \{1,2\}} \dfrac{1}{2} \log_2 \left(\dfrac{h_{j,u}^2 P_u + N}{I_j (\alpha - \beta_j)^2 + N} \right) \ , \\ R_2 & \leq & \dfrac{1}{2} \log_2 \left(\dfrac{g_u^2 P_u + g_v^2 P_v + N}{g_u^2 P_u + N} \right) \ , \end{array} \right. \tag{2.25}$$

where β_j and I_j are given similarly by:

$$\beta_j = \frac{P_u\, h_{j,u}\, h_{j,v}}{h_{j,u}^2\, P_u + N} \quad \text{and} \quad I_j = \left(\frac{P_v}{P_u} \right) \frac{\left(h_{j,u}^2 P_u + N \right)^2}{h_{j,u}^2 P_u + h_{j,v}^2 P_v + N} \, . \tag{2.26}$$

The second rate region is given by the set of rate pairs satisfying:

$$\mathcal{R}_2 : \begin{cases} R_2 & \leq & \frac{1}{2}\log_2\left(\frac{g_v^2 P_v + N}{N}\right) , \\ R_1 & \leq & \min\limits_{j=1,2} \frac{1}{2}\log_2\left(\frac{h_{j,u}^2 P_u + h_{j,v}^2 P_v + N}{h_{j,v}^2 P_v + N}\right) . \end{cases} \tag{2.27}$$

Proposition 5 (CD inner bound)**.** *An inner bound on the capacity region of the Compound MISO BC defined in* (2.16) *is given by the set of rates satisfying:*

$$\mathcal{R}_{\text{CD-MISO BC}} = \bigcup_{\substack{(P_u,P_v) \\ P_u+P_v\leq P}} \bigcup_{\substack{\mathbf{B}_u,\mathbf{B}_v \\ \|\mathbf{B}_u\|=1 \\ \|\mathbf{B}_v\|=1}} \left[\mathcal{R}_1(\mathbf{B}_u,\mathbf{B}_v,P_u,P_v) \cup \mathcal{R}_2(\mathbf{B}_u,\mathbf{B}_v,P_u,P_v)\right] . \tag{2.28}$$

Proof: First, note that the rate regions $\mathcal{R}_1$ and $\mathcal{R}_2$ are nothing but the two corner points of the CD rate region given in (2.2). The rate region $\mathcal{R}_1$ is obtained by evaluating the corner point:

$$\begin{cases} R_1 & \leq & \min\limits_{j\in\{1,2\}} I(U;Y_j|Q) - I(U;V|Q) \\ R_2 & = & I(V;Z|Q) \end{cases} , \tag{2.29}$$

using the following coding scheme:

$$\begin{cases} \mathbf{X} & = & X_u\mathbf{B}_u + X_v\mathbf{B}_v , \\ U & = & X_u + \alpha X_v = X_u + \alpha V , \end{cases} \tag{2.30}$$

where $X_u \sim \mathcal{N}(0,P_u)$ and $X_v \sim \mathcal{N}(0,P_u)$ are independent RVs such that $P_u + P_v \leq P$.

As for the second rate region $\mathcal{R}_2$, it results from the evaluation of the second corner point of CD under the antagonist coding scheme, where V dirty-paper codes the codewords U; the calculations follow in a similar manner. ■

2.2.3 MD-DPC with Uncorrelated Private Descriptions

In the sequel, we will evaluate the MD inner bound given in Theorem 20. To this end, we explore two different approaches for MD-DPC depending on the existing correlation between the private descriptions, for which it will be enough to study the specific corner points:

$$\begin{cases} R_1 & \leq & \min\limits_{j\in\{1,2\}} \Big[I(U_0U_j;Y_j|Q) - I(U_0U_j;V|Q)\Big] \\ 2R_1 & \leq & \sum\limits_{j\in\{1,2\}} \Big[I(U_0U_j;Y_j|Q) - I(U_0U_j;V|Q)\Big] - I(U_1;U_2|U_0VQ) \\ R_2 & = & I(V;Z|Q) . \end{cases} \tag{2.31}$$

The MD inner bound we derive here is based on the evaluation of (2.31) via a time-sharing argument [33], where, unlike the common description, each private description is transmitted only part of the time. Both common and private descriptions apply a DPC

scheme, but with difference parameters and signallings as will be clarified later. Let Q be a binary valued time-sharing RV such that:

$$\mathbb{P}(Q=1) = 1 - \mathbb{P}(Q=2) \triangleq t \ . \tag{2.32}$$

Let us define the following rate region $\mathcal{R}_u$ as:

$$\mathcal{R}_u : \left\{ \begin{array}{rcl} R_1 & \leq & \max\limits_{\alpha} \min\limits_{j\in\{1,2\}} \left\{ \dfrac{1}{2}\, p_Q(j)\, \log_2 \left(\dfrac{h_{j,u}^2\, x + N}{N} \right) \right. \\ & & \left. + \dfrac{1}{2} \log_2 \left(\dfrac{h_{j,u}^2 P_u + N}{I_j^x \left(\alpha - \beta_j^x\right)^2 + N + h_{j,u}^2 x} \right) \right\} , \\ R_2 & \leq & \dfrac{1}{2} \log_2 \left(\dfrac{g_u^2\, P_u + g_v^2\, P_v + N}{g_u^2\, P_u + N} \right) \ , \end{array} \right.$$

where β_j^x and I_j^x are chosen as follows:

$$\beta_j^x = \frac{(P_u - x)\, h_{j,u}\, h_{j,v}}{h_{j,u}^2 P_u + N} \quad \text{and} \quad I_j^x = \left(\frac{P_v}{P_u - x} \right) \frac{\left(h_{j,u}^2 P_u + N \right)^2}{h_{j,u}^2 P_u + h_{j,v}^2 P_v + N} \ . \tag{2.33}$$

Proposition 6 (MD-DPC inner bound with uncorrelated private descriptions)**.** *An inner bound on the capacity region of the Compound MISO BC defined in* (2.16) *is given by:*

$$\mathcal{R}_{\textit{MDindep-MISO BC}} = \bigcup_{t\in[0:1]} \ \bigcup_{\substack{(P_u,,P_v) \\ P_u+P_v\leq P \\ 0\leq x\leq P_u}} \ \bigcup_{\substack{\mathbf{B}_u,\mathbf{B}_v \\ \|\mathbf{B}_u\|=1 \\ \|\mathbf{B}_v\|=1}} \mathcal{R}_u(\mathbf{B}_u, \mathbf{B}_v, x, t, P_u, P_v) \ . \tag{2.34}$$

Proof: For $Q = 1$, we let:

$$\left\{ \begin{array}{rcl} \mathbf{X} & = & (X_u + X_p)\, \mathbf{B}_u + X_v \mathbf{B}_v \ , \\ U_0 & = & X_u + \alpha\, X_v \ , \\ U_2 & = & \emptyset \ , \\ U_1 & = & X_p + \alpha_1\, X_v \ . \end{array} \right. \tag{2.35}$$

And alternately for $Q = 2$, let:

$$\left\{ \begin{array}{rcl} \mathbf{X} & = & (X_u + X_p)\, \mathbf{B}_u + X_v \mathbf{B}_v \ , \\ U_0 & = & X_u + \alpha\, X_v \ , \\ U_1 & = & \emptyset \ , \\ U_2 & = & X_p + \alpha_2\, X_v \ . \end{array} \right. \tag{2.36}$$

In this case, the correlation term becomes null since U_1 and U_2 are never activated in the same time slot. Hence, (2.31) becomes equal to:

$$R_1 \leq I(U_0; Y_1|Q) - I(U_0; V|Q) + t \left[I(U_1; Y_1|U_0, Q{=}1) - I(U_1; V|U_0, Q=1) \right] , \tag{2.37}$$

$$R_1 \leq I(U_0; Y_2|Q) - I(U_0; V|Q) + \bar{t} \left[I(U_2; Y_2|U_0, Q{=}2) - I(U_2; V|U_0, Q=2) \right] , \tag{2.38}$$

$$R_2 \leq I(V;Z|Q) \ . \tag{2.39}$$

The key point is then to note that, for $j \in \{1,2\}$:

$$I(U_0;Y_j|Q) - I(U_0;V|Q) \overset{(a)}{=} \frac{1}{2}\log_2\left(\frac{h_{j,u}^2 P_u + N}{I_j^x\left(\alpha-\beta_j^x\right)^2 + N + h_{j,u}^2 x}\right), \tag{2.40}$$

where (a) is a result of that the CD suffers from the interference of the private description power $h_{j,u}^2 x$ over both time slots in the exact same manner, be it from the private description U_1 or from U_2. Finally, the result follows by using Lemma 1 to maximize the private DPC parameters α_1 and α_2. ■

2.2.4 MD-DPC with Correlated Private Descriptions

In this section, we allow the private descriptions U_1 and U_2 in (2.31) to be arbitrarily correlated. Let the set of rate pairs $\mathcal{R}_c$ defined by:

$$\mathcal{R}_c : \begin{cases} R_1 & \leq & \min\{f_1(\alpha,x), f_2(\alpha,x)\} \ , \\ R_1 & \leq & \frac{1}{2}\left[f_1(\alpha,x) + f_2(\alpha,x) - \frac{1}{2}\log_2(2\pi e x)\right] \ , \\ R_2 & \leq & \frac{1}{2}\log_2\left(\frac{g_u^2 P_u + g_v^2 P_v + N}{g_u^2 P_u + N}\right) \ , \end{cases}$$

where:

$$f_j(\alpha,x) \triangleq \frac{1}{2}\log_2\left(\frac{h_{j,u}^2\, P_u + N}{\dfrac{I_j^x N(\alpha-\beta_j^x)^2}{h_{j,u}^2 x + N} + N}\right) \ , \tag{2.41}$$

and β_j^x and I_j^x are given similarly to (2.22) by:

$$\beta_j^x = \frac{(P_u - x)\, h_{j,u}\, h_{j,v}}{h_{j,u}^2 P_u + N} \quad \text{and} \quad I_j^x = \left(\frac{P_v}{P_u - x}\right)\frac{\left(h_{j,u}^2 P_u + N\right)^2}{h_{j,u}^2 P_u + h_{j,v}^2 P_v + N} \ . \tag{2.42}$$

Proposition 7 (MD inner bound with correlated private descriptions)**.** *An inner bound on the capacity region of the Compound MISO BC is given by:*

$$\mathcal{R}_{\textit{MDcorr-MISO BC}} = \bigcup_{\substack{\mathbf{B}_u,\mathbf{B}_v \\ \|\mathbf{B}_u\|=1 \\ \|\mathbf{B}_v\|=1}} \ \bigcup_{\substack{(P_u,P_v) \\ P_u+P_v\leq P \\ 0\leq x\leq P_u}} \ \bigcup_{\alpha\in\mathbb{R}} \mathcal{R}_c(\mathbf{B}_u,\mathbf{B}_v,\alpha,x,P_u,P_v) \ . \tag{2.43}$$

Proof: To prove our claim, we resort to the MD coding inner bound letting, in the single letter, the two auxiliary rvs be U_1 and U_2 equal given Q, U_0, and V. The correlation term becomes thus:

$$I(U_1;U_2|QU_0V) = H(U_1|QU_0V) = H(U_2|QU_0V) \ . \tag{2.44}$$

Let us use the following coding scheme:

$$\left\{\begin{array}{rcl} \mathbf{X} & = & (X_u + X_p)\mathbf{B}_u + X_v\mathbf{B}_v \ , \\ U_0 & = & X_u + \alpha X_v \ , \\ U_1 & = & X_p + \alpha_1 X_v \ , \\ U_2 & = & X_p + \alpha_2 X_v \ , \\ V & = & X_v \ . \end{array}\right. \tag{2.45}$$

It is then straightforward with the result of Lemma 1, that the achievable rates are those given in the proposition. ■

2.2.5 MD-DPC strictly outperforms CD-DPC

Let us now be in the presence of the most stringent compound model where $\mathbf{h}_1$ and $\mathbf{h}_2$ are unit-norm orthogonal channels. Assume also that the other user's channel is quite accommodating such that $\mathbf{g}$ is orthogonal to the "mean channel" of user 1,

$$\mathbf{g} \perp \frac{1}{\sqrt{2}}(\mathbf{h}_1 + \mathbf{h}_2) = \mathbf{h}_{1,2} \ . \tag{2.46}$$

In order to show that MD-DPC strictly outperforms CD-DPC for this setting, we need to evaluate CD-DPC inner bound based on the corresponding channel models. Then, we show that the MD-DPC inner bound strictly outperforms it.

CD-DPC inner bound

We start by characterizing CD-DPC inner bound in a closed form.

Proposition 8 (CD-DPC inner bound)**.** *The CD-DPC inner bound writes as the set of rate pairs satisfying:*

$$\left\{\begin{array}{rcl} R_1 & \leq & \frac{1}{2}\log_2\left(\frac{P_u + 2N}{P(\eta) + 2N}\right) \ , \\ R_2 & \leq & \frac{1}{2}\log_2\left(\frac{(1-\eta)P_v + 2N}{2N}\right) \ , \end{array}\right. \tag{2.47}$$

for some $\eta \in [-1:1]$*, where*

$$P(\eta) \triangleq \frac{(1-\eta)P_v P_u}{P + 2N + \sqrt{(P+2N)^2 + (\eta^2 - 1)P_v^2}} \ . \tag{2.48}$$

Proof: The proof is relegated to Appendix C.4. ■

Remarks 21. *In order to derive the optimal value of* η *for the overall rate region, we look at the resulting weighted sum-rate. If we let* $\mu \in \Re_+$*, then the optimization of* $R_1 + \mu R_2$ *over* η *depends on the value of* μ*. For* $\mu = 0$*, the optimal choice is* $\eta = 1$ *that is we have to transmit in a direction that is collinear with the mean channel* $\mathbf{h}_{1,2}$*, as for the case* $\mu \to \infty$*, the optimal choice is to let* $\eta = -1$*, which means to transmit the information for the second user in a direction that is collinear to its channel. For intermediate values of* μ*, the weighted sum-rate is not necessarily maximized with either choices of* η*.*

We evaluate the two MD-DPC inner bounds as a function of x, the power dedicated to private descriptions, and compare them to the case $x = 0$, i.e., the CD-DPC inner bound. We let $\mathbf{B}_u = \mathbf{h}_{1,2}$ and thus, by transmitting information to user 1 orthogonal to the channel of user 2.

MD-DPC with correlated private descriptions outperforms CD-DPC

To evaluate the gain of MD-DPC inner bound with *arbitrarily correlated* private descriptions, note that if at least $0 \leq x \leq (2\pi e)^{-1}$, then the bound on R_1 can be written as follows:

$$R_1 \leq \frac{1}{2}\max_{\alpha\in\mathbb{R}} \min\{\, f_1(\alpha, x)\ ,\ f_2(\alpha, x)\} \tag{2.49}$$

$$= \frac{1}{2}\log_2\left(\frac{P_u + 2N}{\dfrac{(P_u - x)}{x + 2N}\dfrac{2N}{P_u}P(\eta) + 2N}\right) \tag{2.50}$$

$$\overset{(a)}{\geq} \frac{1}{2}\log_2\left(\frac{P_u + 2N}{P(\eta) + 2N}\right)\ , \tag{2.51}$$

where (a) follows from the fact that the function $f : x \mapsto \dfrac{(P_u - x)}{x + 2N}$ is strictly decreasing in x. Indeed, the inequality in (a) is strict for non-degenerate power parameters $P_v \neq 0$ and $\eta \neq 1$, which corresponds to $R_2 \neq 0$ and yields the proof of the claim.

MD-DPC with uncorrelated private descriptions outperforms CD-DPC

As for MD-DPC inner bound with *uncorrelated private descriptions*, the constraint on the rate R_1 writes as:

$$R_1 \leq \frac{1}{2}\log_2\left(\frac{P_u + 2N}{\dfrac{(P_u - x)}{\sqrt{x + 2N}}\dfrac{\sqrt{2N}}{P_u}P(\eta) + \sqrt{2N}\,\sqrt{x + 2N}}\right)\ , \tag{2.52}$$

for which we have considered a time-sharing $t = \bar{t} = 0.5$. Now, the function given by

$$g(x) \triangleq \frac{(P_u - x)}{\sqrt{x + 2N}}\frac{P(\eta)}{P_u} + \sqrt{x + 2N}\ , \tag{2.53}$$

is not compulsorily strictly decreasing in x for all values of η. However, it is clear that:

$$g'(x) = \frac{(x + 2N)P(\eta) + (P_u + 2N)(P_u - P(\eta))}{2P_u(x + 2N)^{3/2}}\ , \tag{2.54}$$

and since $0 \leq x \leq P_u$, then:

$$g'(x) \leq \frac{1}{4P_uN\sqrt{2N}}(P_u + 2N)\Big(P_u - 2P(\eta)\Big)\ . \tag{2.55}$$

Thus, $P(\eta) > \frac{P_u}{2}$ suffices to have the function g strictly decreasing in x, and thus, the claim of strict optimality would be proved. Note that if e.g. $P \geq 4N$, then for values of η close to -1, i.e., R_2 close to second user's capacity, the gain is strictly positive and more significant.

Comparison of the MD-DPC inner bounds

An interesting question to investigate is whether the MD inner bound with correlated descriptions outperforms or not the same with uncorrelated descriptions. These two bounds compare differently following the values of the channel gains. The MD with uncorrelated private descriptions makes each user loose:

$$\frac{1}{4}\log_2\left(\frac{\|\mathbf{h}\|^2 x + 2N}{2N}\right) \tag{2.56}$$

compared to the single rates of the MD-DPC with correlated descriptions. Whereas the latter, through the correlation coefficient, engenders a loss of

$$\frac{1}{4}\log_2\left(2\pi e x\right) \ . \tag{2.57}$$

Thus, the relative behavior of these two bounds depends on the specific values of N, P_u and $\|\mathbf{h}\|^2$. In Fig. 2.1, we plot the corresponding rate regions for SNR = 10 dB, $\|\mathbf{h}_1\| = \|\mathbf{h}_2\| = 2$ and the assumptions made on the channels' structure.

2.2.6 Block Expansion

Last, the bounds we have studied so far did not allow for different encoding parameters across time slots. The reason is that the question we were exploring is one of the utility of private descriptions in the Compound MISO BC. Now, if we combine CD inner bound and MD inner bound with correlated private descriptions both with a time-sharing argument where in each time slot, a new coding scheme is used (in terms of beams, power allocations and DPC parameters), then one could expect that the behavior is still captured by the obtained bounds. Fig. 2.2 corroborates the previous statement.

Yet, Block Expansion does not enhance much the performance of MD-DPC coding scheme, the reason being these schemes allow already for good coding schemes, however, CD-DPC is much more enhanced by Block Expansion. Indeed, in the DoF analysis, Time Sharing is crucial for CD-DPC to be DoF optimal [33].

2.2.7 Outer Bound on the Capacity of the Compound MISO BC

In this section, we present an outer bound on the capacity region of the Compound MISO BC which consists in the intersection of some rate regions.

Let us introduce the following channel matrices:

$$\mathbf{g}_{1,2} \triangleq [\mathbf{g}\ \mathbf{h}_1\ \mathbf{h}_2] \ , \tag{2.58}$$

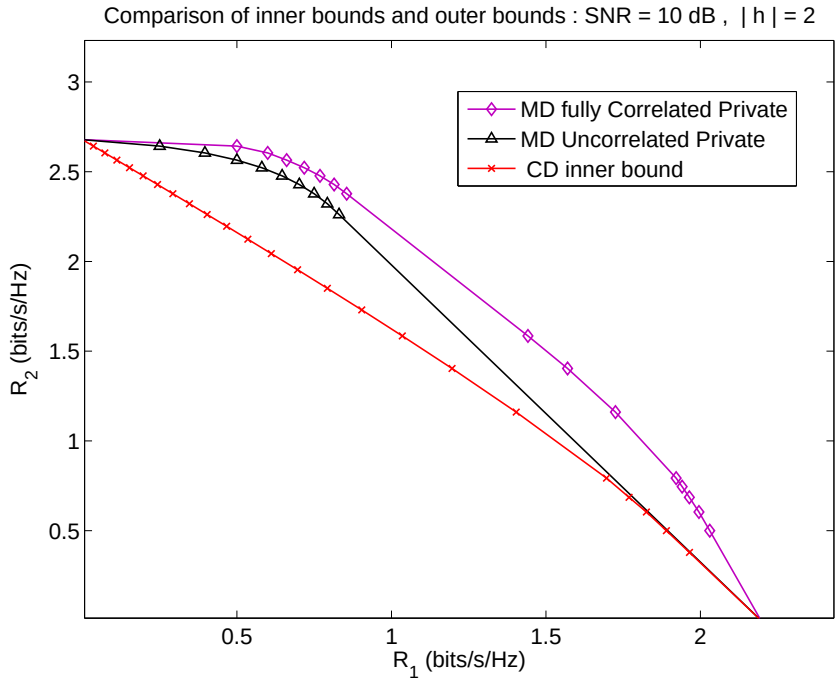


Figure 2.1: Comparison of the CD-DPC and the MD-DPC inner bounds with uncorrelated and correlated private descriptions: SNR = 10 dB, $\|\mathbf{h}_1\| = \|\mathbf{h}_2\| = 2$.

$$\mathbf{h}_{1,z} \triangleq [\mathbf{h}_1 \ \mathbf{g}] \ , \tag{2.59}$$
$$\mathbf{h}_{2,z} \triangleq [\mathbf{h}_2 \ \mathbf{g}] \ . \tag{2.60}$$

We then define the corresponding channel outputs to the channel $\mathbf{g}_{1,2}$, that has the same marginal as the output formed by the concatenation of $[Z \ Y_1 \ Y_2]$, as $Z_{1,2}$, and we define similarly the two outputs $Y_{1,z}$ and $Y_{2,z}$. The following theorem gives the resulting outer bound.

Theorem 22 (Outer bound on the capacity of the Compound MISO BC)**.** *An outer bound on the capacity region of the Compound MISO BC is given by the set of rate pairs:*

$$\mathcal{O} = \mathcal{C}_1 \cap \mathcal{C}_2 \cap \mathcal{C}_{1,2} \cap \mathcal{C}_z \ , \tag{2.61}$$

where $\mathcal{C}_j$ is the capacity region of the BC with outputs (Y_j, Z), for $j \in \{1, 2\}$,

$$\mathcal{C}_j = \bigcup_{\substack{(\mathbf{K}_u, \mathbf{K}_v) \\ tr(\mathbf{K}_u + \mathbf{K}_v) \leq P}} \Bigg\{ (R_1, R_2) \in \mathbb{R}_+^2 \ ,$$
$$R_1 \leq \frac{1}{2} \log_2 \left(\frac{\mathbf{h}_j^t \mathbf{K}_u \mathbf{h}_j + N}{N} \right) \tag{2.62}$$
$$R_2 \leq \frac{1}{2} \log_2 \left(\frac{\mathbf{g}^t (\mathbf{K}_u + \mathbf{K}_v) \mathbf{g} + N}{\mathbf{g}^t \mathbf{K}_u \mathbf{g} + N} \right) \tag{2.63}$$
$$or$$

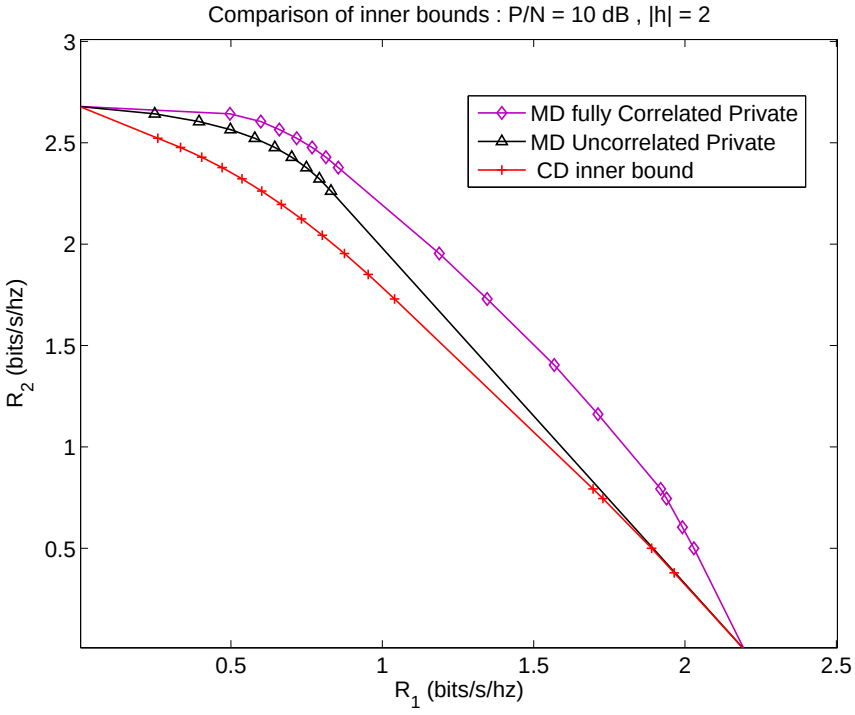


Figure 2.2: Comparison of the CD-DPC and MD-DPC with uncorrelated and correlated private descriptions inner bounds with a time-sharing argument: SNR = 10 dB, $\|\mathbf{h}_1\| = \|\mathbf{h}_2\| = 2$.

$$R_1 \leq \frac{1}{2}\log_2\left(\frac{\mathbf{h}_j^t(\mathbf{K}_u+\mathbf{K}_v)\mathbf{h}_j+N}{\mathbf{h}_j^t\mathbf{K}_v\mathbf{h}_j+N}\right) \tag{2.64}$$

$$R_2 \leq \frac{1}{2}\log_2\left(\frac{\mathbf{g}^t\mathbf{K}_v\mathbf{g}+N}{N}\right)\Bigg\}\,, \tag{2.65}$$

$\mathcal{C}_{1,2}$ is the capacity region of the Compound MISO BC with outputs $(Y_1, Z_{1,2})$ and $(Y_2, Z_{1,2})$,

$$\mathcal{C}_{1,2} = \bigcup_{\substack{(\mathbf{K}_u,\mathbf{K}_v)\\ tr(\mathbf{K}_u+\mathbf{K}_v)\leq P}} \Bigg\{(R_1,R_2)\in\mathbb{R}_+^2\,,$$

$$R_1 \leq \min_{j\in\{1,2\}}\frac{1}{2}\log_2\left(\frac{\mathbf{h}_j^t(\mathbf{K}_u+\mathbf{K}_v)\mathbf{h}_j+N}{\mathbf{h}_j^t\mathbf{K}_v\mathbf{h}_j+N}\right)\,, \tag{2.66}$$

$$R_2 \leq \frac{1}{2}\log_2\left(\frac{\left|\mathbf{g}_{1,2}^t\mathbf{K}_v\mathbf{g}_{1,2}+N\mathbf{I}_3\right|}{N^3}\right)\Bigg\} \tag{2.67}$$

and finally, $\mathcal{C}_z$ is the capacity region of the Compound BC with outputs $(Y_{1,z}, Z)$ and $(Y_{2,z}, Z)$,

$$\mathcal{C}_z = \bigcup_{\substack{(\mathbf{K}_u,\mathbf{K}_v)\\ tr(\mathbf{K}_u+\mathbf{K}_v)\leq P}} \Bigg\{(R_1,R_2)\in\mathbb{R}_+^2\,,$$

$$R_1 \leq \min_{j\in\{1,2\}} \frac{1}{2}\log_2\left(\frac{\left|\mathbf{h}_{j,z}^t \mathbf{K}_u \mathbf{h}_{j,z} + N\mathbf{I}_2\right|}{N^2}\right) \tag{2.68}$$

$$R_2 \leq \frac{1}{2}\log_2\left(\frac{\mathbf{g}^t(\mathbf{K}_u + \mathbf{K}_v)\mathbf{g} + N}{\mathbf{g}^t\mathbf{K}_u\mathbf{g} + N}\right)\Bigg\} . \tag{2.69}$$

Proof: The proof is straightforward from the following observations. The fact that the capacity of the considered compound model is always included in the intersection of the capacities of the BCs $\mathcal{C}_1$ and $\mathcal{C}_2$, and that this setting is a degraded version of the setups where there is a least one user with an extra receive antenna, whose capacities are given in references [39], [40]. ■

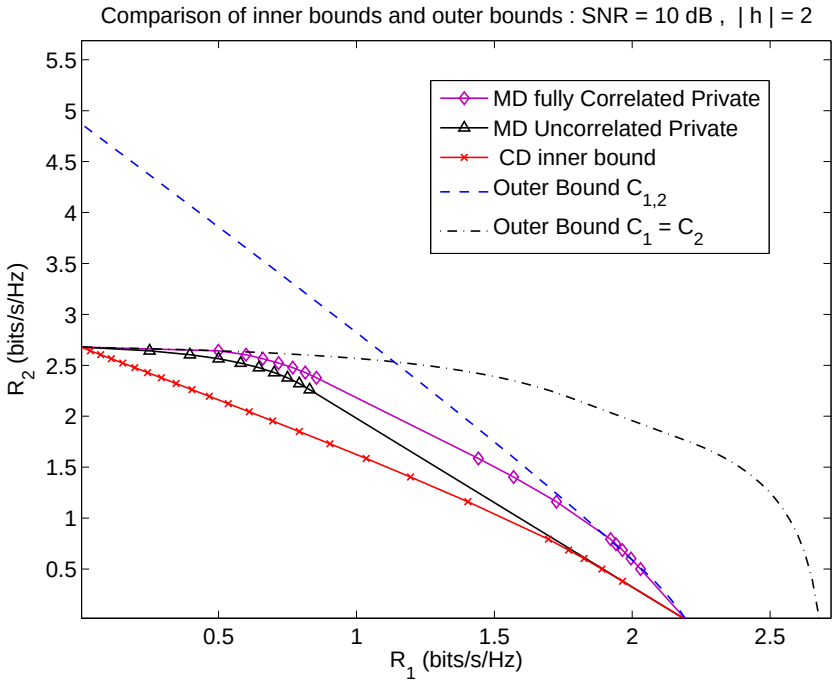


Figure 2.3: Comparison of the inner bounds and the intersection of the outer bounds: SNR = 10 dB, $\|\mathbf{h}_1\| = \|\mathbf{h}_2\| = 2$.

Remarks 23. *The outer bound stated in Theorem 22 is tight in the high SNR regime and thus is DoF optimal. To check this, notice that the bounds $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{C}_z$ attain each the points $(d_1 \leq 1\ ,\ d_2 \leq 1)$ by letting $\mathbf{K}_u = \mathbf{g}^\perp \times (\mathbf{g}^\perp)^t$. As for the bound $\mathcal{C}_{1,2}$, it achieves all the points $(2d_1 + d_2 \leq 2)$, thus the intersection of these two regions leads to the optimal DoF.*

In Fig. 2.3, we plot the inner and outer bound for intermediate SNR values. Although the gap with the outer bound suggests that the inner and outer regions do not meet, it is our belief that the inner bound is tight while our outer remains rather loose.

Summary

In this first part of the thesis, we explored novel decoding and encoding technique for the two-user memoryless Compound BC.

We first studied the role of Interference Decoding (ID) where an achievable rate region is derived via *superposition coding* and *random binning*. At the decoders, the constraint of decoding only the intended message is alleviated to allow each of the users to decode or not the other user's (interference) message. Unlike for the standard two-user BC, this strategy proves to be useful in compound setups, where channel uncertainty prevents the encoder from coding optimally for each possible BC formed by all pairs of channels in the set. A simple outer bound is also derived based on the best outer bound hitherto known on the capacity region of the two-user BC. This outer bound captures one of the most stringent effects of simultaneity of users over the random codes constructed: antagonist coding strategies. Surprisingly enough, ID not only outperforms Non-Interference Decoding (NID) technique, i.e., Marton's worst-case rate region, but also allows to achieve the capacity of a class of relevant BC while NID stays strictly suboptimal. Thus, though the coding scheme is simple (in terms of the number of auxiliary variables involved and of the complexity of the encoding operation) the decoders' optimization allows to palliate the uncertainty at the source.

Later, we studied an encoding technique with a more evolved coding strategy, namely Multiple Description (MD) coding. The source transmits to the group of users, interested in the same message, common and private descriptions. For the specific case of the Compound MISO BC, resorting to MD is essential since a common description, i.e., applying DPC with a single description cannot accommodate the interference seen by each instance of the users channels in the set, unless combining it with a time-sharing argument. The key point in the MISO BC setting is that using a fraction of power to transmit the private descriptions is useful for all SNR ranges while turns out to be DoF optimal. Indeed, each private description creates an interference free link and thus each user can recover a part of its rate interference free. Though, unlike in the ID analysis part, we could not perform an optimization of the Common Description inner bound, Marton's inner bound, which is known to be a very hard problem with the existing tools to date, we carried out an involved optimization of the CD-DPC inner bound to prove the limitation of such a common-description-based coding.

Both these strategies (Interference Decoding and Multiple Description coding) prove to be strictly useful in compound settings as they allow each of the users (in the compound set) to deal with interference in a dedicated manner.

Part II

The Multicast Cognitive Interference Channel

Introduction and Setup

1 Introduction

The Cognitive Interference Channel (CIFC) in Fig. 1 was first introduced by Devroye et.al [6] as an interference channel with two sources and two destinations but where one of the sources has full non causal knowledge of both messages to be transmitted. The cognitive source models the secondary transmitter of a cognitive radio environment, that upon sensing the primary transmitter's message, communicates the secondary message to the secondary user. As such, the secondary source should not create too much interference in the secondary transmission so as not to cause impediment to the primary communication, however, it can also cooperate with the primary source and thus enhance the performances of the primary communication. As it is defined, a CIFC can be regarded as a Broadcast Channel with a helper (the primary source). The helper enhances the transmission of the message W_1 in the BC formed by X_2 and the two destinations (Y, Z), however, it creates more interference at user Z that is interested only in message W_2. The optimal transmission strategy for such a setting is hitherto unknown, however,a few cases have been solved in literature.

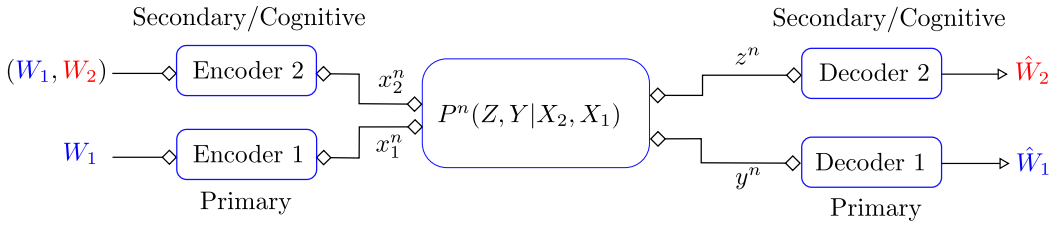


Figure 1: Cognitive Interference Channel

The first capacity result of this setting is due to Maric *et.al* [7] for the "very strong interference" regime based on an equivalence with the Interference Channel (IFC) with a common message. Later Wu *et al* in [8], and independently Jovicic in [17], characterized the capacity region of the "very weak interference" regime. The capacity of the Z-CIFC with a noiseless link was derived by Liu *et.al* in [18] and the classes of less noisy and more capable CIFC were investigated in the works of Vaezi [19] [20]. All inner bounds suggested in these works were dedicated to the setting investigated and failed most in encompassing all existing inner bounds. Lately, a work by Rini *et.al* proposed in [26] a unifying inner bound that is capacity achieving in all regimes in which capacity is known, through a

combination of known techniques of binning, rate splitting, and superposition coding. They also suggest a new outer bound that alleviates the computational complexity of existing outer bounds that involve auxiliary random variables. Based on the proposed inner bound, the capacity region of a new regime, denoted as " better cognitive decoding (BCD)" regime, was derived along with the capacity of the semi-deterministic CIFC.

As for the Gaussian CIFC, the entire capacity region remains to be fully characterized, yet, some regimes are fully understood: the weak interference capacity region was derived in [8] while that of the very strong interference was derived in [7] and that of the "primary decodes interference" regime was found in [45]. The S-CIFC, where interference is experienced only on the primary user's side, was also extensively studied and the capacity region in the weak interference was characterized under different strong interference regimes by Jiang *et.al* in [46], Vaezi *et.al* in [47], and Rini *et.al* in [45].

In this work, we investigate the N-multicast CIFC, Fig. 2 where many primary users are interested in the same message and where there is only one secondary transmitter. A

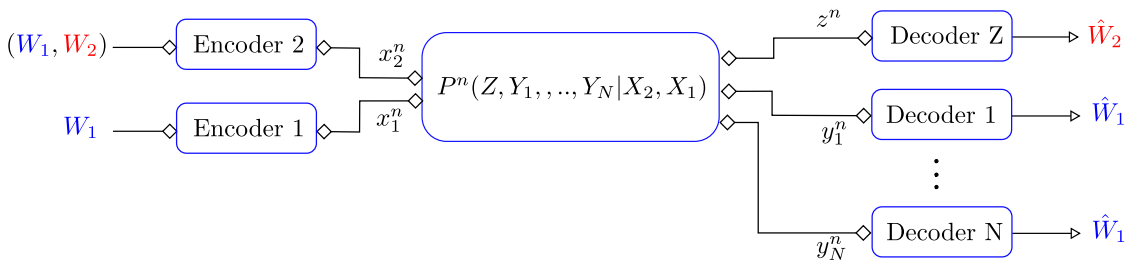


Figure 2: The Multicast Cognitive Interference Channel / Broadcast Channel with a helper and a common message

possible deployment scenario consists of several users (spectators) in a football stadium being able to have access to instantaneous replay of the most important scenes on their cell phone while a nearby base station helps with the communication.

We start by deriving an inner bound on the capacity region of this setting, which combines the optimal coding techniques of the *Broadcast Channel* (superposition coding and random binning) with rate-splitting for the *Interference Channel*. This inner bound recovers Marton's inner bound in the absence of the primary user. Then, we evaluate this rate region in both cases of very strong interference, very weak interference, showing that the respective rate regions are both converse and thus achieve the capacity region. Later, we characterize also the capacity region of the mixed weak/ strong interference regime where among the multicast set of users, those users that are in very weak interference regime decode only their useful signals while those experiencing strong interference decode the interfering message as well, i.e Interference Decoding scheme. Last but not least, we fully characterize the capacity region of the corresponding Gaussian cases resorting to standard upper bounding techniques and Gaussian signalling arguments.

2 Problem Definition

The discrete memoryless N-Multicast CIFC can be represented by the conditional pmf:

$$P_{Z^n Y_1^n \cdots Y_N^n | X_1^n X_2^n} = \prod_{i=1}^{n} P_{Z_i Y_{1,i} \cdots Y_{N,i} | X_{1,i} X_{2,i}} \ . \tag{1}$$

An (M_{1n}, M_{2n}, n)-code for this channel consists of: two sets of messages, $\mathcal{M}_1$ and $\mathcal{M}_2$, two encoding functions, and $N+1$ decoding functions. The encoding function at source 1 (the primary source) assigns an n-sequence $x_1^n(W_1)$ to each message W_1, and the encoding function at source 2 assigns an n-sequence $x_2^n(W_1, W_2)$ to each pair of messages $(W_1, W_2) \in \mathcal{M}_1 \times \mathcal{M}_2$. The secondary decoder assigns to each received sequence Z^n an estimate message $\hat{W}_2$ while the primary decoders each resort to a decoding function that assigns to each received sequence Y_j^n, an estimate message $\hat{W}_{1,j}$, $j \in [1:N]$.

The probability of error is given by:

$$P_e^{(n)} \triangleq \mathbb{P}\left(\hat{W}_2 \neq W_2 \text{ or } \bigcup_{j \in [1:N]} \hat{W}_{1,j} \neq W_1 \right). \tag{2}$$

A rate pair (R_1, R_2) is said to be achievable if there exists an (M_{1n}, M_{2n}, n)-code satisfying:

$$\liminf_{n \to \infty} \frac{1}{n} \log_2 M_{kn} \geq R_k \quad \forall\, k = \{1, 2\}\,, \tag{3}$$

$$\limsup_{n \to \infty} P_e^{(n)} = 0. \tag{4}$$

The convex closure over all achievable rate pairs (R_1, R_2) defines the capacity region.

Chapter 3

Capacity results for the Multicast CIFC

In this part of the thesis, we derive capacity results for the Multicast CIFC. The focus is on whether we can extend the capacity results of the CIFC to the multicast case, and to what extent. Our answer is positive in most cases, however it requires a thorough investigation and alternative proofs of the existing results on the CIFC to extend them to the multicast setting.

3.1 Inner bound on the capacity region of the Multicast CIFC

Consider the channel model in Fig. 1. .

In this section, we derive an inner bound on the capacity region of the CIFC, that generalizes Marton's inner bound for the BC in the presence of a helper.

Theorem 24. *An inner bound on the capacity region of the CIFC consists in all rate pairs* (R_1, R_2) *satisfying:*

$$R_1 \leq \min_{j\in[1:N]} I(Q_1X_1QU;Y_j) \tag{3.1a}$$
$$R_2 \leq I(QV;Z|Q_1) - I(QV;X_1|Q_1) \tag{3.1b}$$
$$R_2 \leq \min_{j\in[1:N]} I(X_1U;Y_j|Q_1Q) + I(QV;Z|Q_1) - I(V;X_1U|Q_1Q) \tag{3.1c}$$
$$R_2 \leq \min_{j\in[1:N]} I(X_1QU;Y_j|Q_1) + I(V;Z|Q_1Q) - I(V;X_1U|Q_1Q) \tag{3.1d}$$
$$R_2 \leq \min_{j\in[1:N]} I(X_1QU;Y_j|Q_1) + I(QV;Z|Q_1) - I(V;X_1U|Q_1Q) - I(Q;X_1|Q_1) \tag{3.1e}$$
$$R_1 + R_2 \leq \min_{j\in[1:N]} I(X_1U;Y_j|Q_1Q) + I(Q_1QV;Z) - I(V;X_1U|Q_1Q) \tag{3.1f}$$
$$R_1 + R_2 \leq \min_{j\in[1:N]} I(Q_1X_1QU;Y_j) + I(V;Z|Q_1Q) - I(V;X_1U|Q_1Q) \tag{3.1g}$$
$$R_1 + R_2 \leq \min_{j\in[1:N]} I(Q_1X_1QU;Y_j) + I(QV;Z|Q_1) - I(V;X_1U|Q_1Q) - I(Q;X_1|Q_1) \tag{3.1h}$$
$$R_1 + R_2 \leq \min_{j\in[1:N]} I(X_1QU;Y_j|Q_1) + I(Q_1QV;Z) - I(V;X_1U|Q_1Q) - I(Q;X_1|Q_1) \tag{3.1i}$$

$$R_1 + 2R_2 \leq \min_{j\in[1:N]} I(X_1QU;Y_j|Q_1) + I(Q_1QV;Z) + I(V;Z|Q_1Q) - I(V;X_1U|Q_1Q) - I(Q;X_1|Q_1) \quad (3.1j)$$

$$R_1 + 2R_2 \leq \min_{j\in[1:N]} I(Q_1X_1QU;Y_j) + I(QV;Z|Q_1) + I(V;Z|Q_1Q) - I(V;X_1U|Q_1Q) - I(Q;X_1|Q_1)\ , \quad (3.1k)$$

for some joint p.m.f $P_{Q_1X_1QUVX_2}$ *satisfying* $(Q_1QUV) \multimap (X_1,X_2) \multimap (Y_1,\cdots,Y_N,Z)$

Remarks 25. *In the absence of the helper, i.e when* $X_1 = Q_1 = \emptyset$*, the inner bound collapses to Marton's inner bound in the multicast setting with the common auxiliary rv* Q *and the two private ones* U *and* V*.*

The variables X_1 *and* Q_1 *account for rate splitting at the primary source. The rate splitting at the secondary source is already contained in Marton's coding with the common auxiliary* Q*.*

Thus, this inner bound combines both optimal coding schemes for the Broadcast Channel and Interference Channel.

Proof. Proof is relegated to appendix D.1.

3.2 Outer bounds on the capacity region of the N-multicast CIFC

In this section, we introduce an outer bound for the N-multicast CIFC relying on an argument from [26] but that we adapt for the N-users case. Later, we show a possible way of improving this outer bound by introducing extra constraints.

Let $Y_1'\cdots Y_N'$ be N channel outputs arbitrarily correlated to Z conditioned on X_1X_2 but that maintain the conditional marginals of $Y_1,\cdots,Y_N$ unchanged, i.e

$$\forall j \in [1:N] \quad P_{Y_j'|X_1X_2} = P_{Y_j|X_1X_2}\ . \quad (3.2)$$

One can then state the following result:

Theorem 26. *An outer bound on the capacity region of the two-multicast CIFC is given by the set of rate pairs that satisfy for some* $P_{X_1X_2}$*:*

$$\begin{cases} R_1 \leq \min_{j\in[1:N]} I(X_1X_2;Y_j)\ , \\ R_2 \leq I(X_2;Z|X_1)\ , \\ R_1+R_2 \leq \min_{j\in[1:N]} \Big[I(X_1X_2;Y_j) + I(X_2;Z|Y_j'X_1)\Big]\ . \end{cases} \quad (3.3)$$

Proof. Let $j \in [1:N]$. We start by Fano's inequality writing that:

$$n\,(R_1-\epsilon_n) = H(W_1) - n\,\epsilon_n \quad (3.4)$$

$$\leq I(W_1;Y_j^n) \quad (3.5)$$

$$\leq I(W_1W_2;Y_j^n) \quad (3.6)$$

$$\leq I(X_1^n X_2^n; Y_j^n) \tag{3.7}$$
$$\leq \sum_{i=1}^{n} I(X_{1,i} X_{2,i}; Y_{j,i}) \ , \tag{3.8}$$
$$n\,(R_2 - \epsilon_n) = H(W_2) - n\,\epsilon_n \tag{3.9}$$
$$\leq I(W_2; Z^n | W_1) \tag{3.10}$$
$$\leq I(X_2^n; Y_j^n | X_1^n) \tag{3.11}$$
$$\leq \sum_{i=1}^{n} I(X_{2,i}; Z_i | X_{1,i}) \ . \tag{3.12}$$

Plus, the sum rate can be bounded as:

$$n\ (R_1 + R_2 - \ \epsilon_n) \leq I(W_1; Y_j^n) + I(W_2; Z^n | W_1) \tag{3.13}$$
$$\leq I(W_1; Y_j^n) + I(W_2; Z^n Y_j'^n | W_1) \tag{3.14}$$
$$\leq I(W_2; Z^n | Y_j'^n W_1) + I(W_2; Y_j'^n | W_1) + I(W_1; Y_1^n) \ . \tag{3.15}$$

The first term $I(W_2; Z^n | \tilde{Y}_j^n W_1)$ can be bounded as follows:

$$I(W_2; Z^n | Y_j'^n W_1) \leq I(X_2^n; Z^n | Y_j'^n X_1^n) \tag{3.16}$$
$$= \sum_{i=1}^{n} I(X_2^n; Z_i | Y_j'^n X_1^n Z^{i-1}) \tag{3.17}$$
$$= \sum_{i=1}^{n} \Big[H(Z_i | Y_j'^n X_1^n Z^{i-1}) - H(Z_i | Y_j'^n X_1^n X_2^n Z^{i-1}) \Big] \tag{3.18}$$
$$\leq \sum_{i=1}^{n} \Big[H(Z_i | Y'_{j,i} X_{1,i}) - H(Z_i | Y'_{j,i} X_{1,i} X_{2,i}) \Big] \tag{3.19}$$
$$= \sum_{i=1}^{n} I(X_{2,i}; Z_i | Y'_{j,i} X_{1,i}) \ . \tag{3.20}$$

The remaining term can be bounded as:

$$I(W_2; Y_j'^n | W_1) + I(W_1; Y_j^n)$$
$$\leq I(X_2^n; Y_j'^n | X_1^n) + I(X_1^n; Y_j^n) \tag{3.21}$$
$$= I(X_2^n; Y_j^n | X_1^n) + I(X_1^n; Y_j^n) \tag{3.22}$$
$$\leq I(X_1^n X_2^n; Y_j^n) \tag{3.23}$$
$$\leq \sum_{i=1}^{n} I(X_{1,i} X_{2,i}; Y_{j,i}) \ . \tag{3.24}$$

This ends our proof. □

Improvement of the outer bound for the 2-Multicast CIFC

Let similarly $\tilde{Y}_1$ and $\tilde{Y}_2$ be two other channel outputs similarly defined as conserving the conditional marginals of Y_1 and Y_2 though arbitrarily correlated to Z conditioned on $(X_1 X_2)$.

One can further improve the outer bound by the following result.

Theorem 27. *An outer bound on the capacity region of the two-multicast CIFC is given by the set of rate pairs that satisfy for some $P_{X_1X_2}$:*

$$\begin{cases} R_1 \leq \min\{I(X_1X_2;Y_1)\ ,\ I(X_1X_2;Y_2)\}\ , \\ R_2 \leq I(X_2;Z|X_1)\ , \\ R_1+R_2 \leq I(X_1X_2;Y_1)+I(X_2;Z|Y_1'X_1)\ , \\ R_1+R_2 \leq I(X_1X_2;Y_2)+I(X_2;Z|Y_2'X_1)\ , \\ 2R_1+R_2 \leq I(X_1X_2;Y_1)+I(X_1X_2;Y_2)+I(X_2;Z|\tilde{Y}_1\tilde{Y}_2X_1)+I(\tilde{Y}_1;\tilde{Y}_2|X_1X_2)\ , \end{cases} \tag{3.25}$$

Proof. The proof of the single and sum rate constraints was already discussed, thus, we show only the bound on $2R_1+R_2$.

We start by Fano's inequality writing that:

$$n\,(2R_1-\epsilon_n) = H(W_1)+H(W_1) \leq I(W_1;Y_1^n)+I(W_1;Y_2^n)\ , \tag{3.26}$$

$$n\,(R_2-\epsilon_n) = H(W_2) \leq I(W_2;Z^nW_1) = I(W_2;Z^n|W_1)\ . \tag{3.27}$$

Thus, the weighted sum rate can be bounded as:

$$n\ (2R_1+R_2-\epsilon_n) \leq I(W_1;Y_1^n)+I(W_1;Y_2^n)+I(W_2;Z^n|W_1) \tag{3.28}$$

$$\leq I(W_1;Y_1^n)+I(W_1;Y_2^n)+I(W_2;Z^n\tilde{Y}_1^n\tilde{Y}_2^n|W_1) \tag{3.29}$$

$$\leq I(W_2;Z^n|\tilde{Y}_1^n\tilde{Y}_2^nW_1)+I(W_2;\tilde{Y}_1^n\tilde{Y}_2^n|W_1)+I(W_1;Y_1^n)+I(W_1;Y_2^n) \tag{3.30}$$

The first term $I(W_2;Z^n|\tilde{Y}_1^n\tilde{Y}_2^nW_1)$ can be bounded as follows:

$$I(W_2;Z^n|\tilde{Y}_1^n\tilde{Y}_2^nW_1) \leq I(X_2^n;Z^n|\tilde{Y}_1^n\tilde{Y}_2^nX_1^n) \tag{3.31}$$

$$= \sum_{i=1}^{n} I(X_2^n;Z_i|\tilde{Y}_1^n\tilde{Y}_2^nX_1^nZ^{i-1}) \tag{3.32}$$

$$= \sum_{i=1}^{n} \Big[H(Z_i|\tilde{Y}_1^n\tilde{Y}_2^nX_1^nZ^{i-1}) - H(Z_i|\tilde{Y}_1^n\tilde{Y}_2^nX_1^nX_2^nZ^{i-1})\Big] \tag{3.33}$$

$$\leq \sum_{i=1}^{n} \Big[H(Z_i|\tilde{Y}_{1,i}\tilde{Y}_{2,i}X_{1,i}) - H(Z_i|\tilde{Y}_{1,i}\tilde{Y}_{2,i}X_{1,i}X_{2,i})\Big] \tag{3.34}$$

$$= \sum_{i=1}^{n} I(X_{2,i};Z_i|\tilde{Y}_{1,i}\tilde{Y}_{2,i}X_{1,i})\ . \tag{3.35}$$

The remaining term can be bounded as:

$$\begin{aligned} &I(W_2;\tilde{Y}_1^n\tilde{Y}_2^n|W_1)+I(W_1;Y_1^n)+I(W_1;Y_2^n) \\ &= H(\tilde{Y}_1^n\tilde{Y}_2^n|W_1)-H(\tilde{Y}_1^n\tilde{Y}_2^n|W_1W_2)+I(W_1;Y_1^n)+H(Y_2^n)-H(Y_2^n|W_1) && (3.36)\\ &= H(\tilde{Y}_1^n|\tilde{Y}_2^nW_1)-H(\tilde{Y}_1^n\tilde{Y}_2^n|W_1W_2)+H(Y_1^n)-H(Y_1^n|W_1)+H(Y_2^n) && (3.37)\\ &= H(\tilde{Y}_1^n|\tilde{Y}_2^nW_1)-I(\tilde{Y}_1^n;\tilde{Y}_2^n|W_1W_2)+H(\tilde{Y}_1^n|W_1W_2)+H(\tilde{Y}_2^n|W_1W_2)+H(Y_1^n) \\ &\qquad -H(Y_1^n|W_1)+H(Y_2^n) && (3.38)\\ &= H(\tilde{Y}_1^n|\tilde{Y}_2^nW_1)+I(\tilde{Y}_1^n;\tilde{Y}_2^n|W_1W_2)-H(\tilde{Y}_1^n|W_1W_2)-H(\tilde{Y}_2^n|W_1W_2)+H(Y_1^n) \\ &\qquad -H(Y_1^n|W_1)+H(Y_2^n) && (3.39) \end{aligned}$$

$$= -I(\tilde{Y}_1^n;\tilde{Y}_2^n|W_1) + I(\tilde{Y}_1^n;\tilde{Y}_2^n|X_1^nX_2^n) + I(X_1^nX_2^n;Y_1^n) + I(X_1^nX_2^n;Y_2^n) \tag{3.40}$$

$$\leq \sum_{i=1}^{n}\Big[I(\tilde{Y}_{1,i};\tilde{Y}_{2,i}|X_{1,i}X_{2,i}) + I(X_{1,i}X_{2,i};Y_{1,i}) + I(X_{1,i}X_{2,i};Y_{2,i})\Big] \ . \tag{3.41}$$

□

This outer bound has the advantage of being easy to compute in the Gaussian case.

3.3 Capacity region of the N-multicast CIFC in the very strong interference regime

In this part of the work, we derive the capacity region of the N-multicast CIFC setting in the very strong interference regime.

To this end, consider the multicast CIFC of Fig 2. We define the strong interference condition as:

$$\forall P_{X_1X_2} \qquad I(X_2;Z|X_1) \leq \min_{j\in[1:N]} I(X_2;Y_j|X_1) \ . \tag{3.42}$$

The very strong interference condition is to further satisfy:

$$\forall P_{X_1X_2} \qquad \min_{j\in[1:N]} I(X_1X_2;Y_j) \leq I(X_1X_2;Z) \ . \tag{3.43}$$

Under the very strong interference condition, we show the following.

Theorem 28 (Very strong interference)**.** *The capacity region of the multicast CIFC satisfying* (3.42) *and* (3.43) *is given by the set of rate pairs* (R_1, R_2) *that satisfy:*

$$\begin{cases} R_2 & \leq & I(X_2;Z|X_1) \ , \\ R_1+R_2 & \leq & \min\limits_{j\in[1:N]} I(X_1X_2;Y_j) \ . \end{cases} \tag{3.44}$$

for some arbitrarily correlated (X_1, X_2)*.*

Proof. The proof of converse follows similar lines as those in [7] and relies on the fact of showing that (3.42) implies that for all P_u s.t $U \multimap (X_1, X_2) \multimap (Z, Y_1, \cdots, Y_N)$:

$$\forall j \in [1:N] \qquad I(X_2^n;Z^n|X_1^nU) \leq I(X_2^n;Y_j^n|X_1^nU) \ . \tag{3.45}$$

Thus, one can write that:

$$n(R_2-\epsilon_n) \leq I(W_2;Z^n|W_1) \tag{3.46}$$

$$\leq I(X_2^nW_2;Z^n|X_1^nW_1) \tag{3.47}$$

$$\leq \sum_{i=1}^{n} I(X_2^nW_2;Z_i|Z^{i-1}X_1^nW_1) \tag{3.48}$$

$$= \sum_{i=1}^{n}\Big[H(Z_i|Z^{i-1}X_1^nW_1) - H(Z_i|Z^{i-1}X_2^nX_1^nW_2W_1)\Big] \tag{3.49}$$

$$\leq \sum_{i=1}^{n}\Big[H(Z_i|X_{1,i}) - H(Z_i|X_{2,i}X_{1,i})\Big] \tag{3.50}$$

$$= \sum_{i=1}^{n} I(X_{2,i}; Z_i | X_{1,i}) \ . \tag{3.51}$$

Moreover, we can write that:

$$\begin{aligned} n(R_1 + R_2 - \epsilon_n) &\leq I(W_1; Y_j^n) + I(W_2; Z^n | W_1) && (3.52)\\ &\leq I(W_1 X_1^n; Y_j^n) + I(X_2^n; Z^n | X_1^n W_1) && (3.53)\\ &\overset{(a)}{\leq} I(W_1 X_1^n; Y_j^n) + I(X_2^n; Y_j^n | X_1^n W_1) && (3.54)\\ &= \sum_{i=1}^{n} I(X_{1,i} X_{2,i}; Y_{j,i}) \ , && (3.55) \end{aligned}$$

where (a) is a consequence of applying inequality (3.45).

The proof of achievability follows from rate region (3.1) letting $Q_1 = X_1$ that is the user Z decodes all interference X_1 and letting $Q = U = V = X_2$ that is applying a simple point to point code at source 2 and letting user 1 decode the whole useful signal X_2. The obtained rate region is of the form:

$$\begin{aligned} R_1 &\leq \min_{j \in [1:N]} I(X_1 X_2; Y_j) \ , && (3.56a)\\ R_2 &\leq I(X_2; Z | X_1) \ , && (3.56b)\\ R_2 &\leq \min_{j \in [1:N]} I(X_2; Y_j | X_1) \ , && (3.56c)\\ R_1 + R_2 &\leq I(X_1 X_2; Z) \ , && (3.56d)\\ R_1 + R_2 &\leq \min_{j \in [1:N]} I(X_1 X_2; Y_j) \ . && (3.56e) \end{aligned}$$

One can notice that (3.56a) is redundant due to the sum rate (3.56e) while (3.56c) is redundant due the strong interference condition (3.42) and (3.56d) is redundant by the very strong interference condition (3.43). □

3.4 Capacity region of the N-multicast CIFC in the very weak interference regime

In this section, we give the capacity region of the setting of weak interference regime as will be defined later.

The way to prove the capacity region of a standard -non multicast CIFC- in the weak interference regime, requires the use at the converse of Csiszár & Körner's identity, thus preventing the extension of the outer bound to the N-multicast CIFC case.

In the sequel, we make use of another outer bound that palliates this difficulty, and that can be extended to an arbitrary number of users in the multicast setting. We first state our outer bound and the conditions under which it applies, and then enunciate the capacity region and prove its achievability later.

Theorem 29 (Weak Interference Outer Bound)**.** *The capacity region of the N-multicast CIFC that verifies the weak interference condition:*

$$\forall j \in [1:N] \ , \ \forall P_{U X_1 X_2} \ , \quad I(U; Y_j | X_1) \leq I(U; Z | X_1) \ , \tag{3.57}$$

is included in the set of rate pairs that satisfy:

$$\begin{cases} R_1 & \leq & \min\limits_{j\in[1:N]} I(UX_1;Y_j) \ , \\ R_2 & \leq & I(X_2;Z|X_1U) \ , \end{cases} \tag{3.58}$$

for some arbitrarily correlated (U, X_1, X_2) *s.t* $U \multimap (X_1, X_2) \multimap (Z, Y_1, \cdots, Y_N)$.

Proof. Let $j \in [1 : N]$. We have by Fano's inequality that:

$$\begin{aligned} n(R_2 - \epsilon_n) &\leq I(W_2; Z^n|W_1X_1^n) && (3.59)\\ &\leq I(X_2^n; Z^n|W_1X_1^n) && (3.60)\\ &= \sum_{i=1}^{n} I(X_2^n; Z_i|Z^{i-1}W_1X_1^n) && (3.61)\\ &\leq \sum_{i=1}^{n} I(X_{2,i}; Z_i|U_iX_{1,i}) \ , && (3.62) \end{aligned}$$

where $U_i = W_1X_1^{i-1}X_{1,i+1}^n Z^{i-1}$.

Now on the other side,

$$\begin{aligned} n(R_1 - \epsilon_n) &\leq I(W_1X_1^n; Y_j^n) && (3.63)\\ &= \sum_{i=1}^{n} I(W_1X_1^nY_j^{i-1}; Y_{j,i}) \ . && (3.64) \end{aligned}$$

The main idea here is that, we can upper bound this expression letting Z^{i-1} replace Y_j^{i-1}, i.e

$$\forall i \in [1 : n] \quad , \quad I(W_1X_1^nY_j^{i-1}; Y_{j,i}) \leq I(W_1X_1^nZ^{i-1}; Y_{j,i}) \ . \tag{3.65}$$

This is due to the conditional less-noisiness of Y_j compared to Z given X_1 (3.57) and it can be proved following similar lines as in [48]:

$$\begin{aligned} & I(W_1X_1^nZ^{i-1}; Y_{j,i}) - I(W_1X_1^nY_j^{i-1}; Y_{j,i}) \\ &= I(Z^{i-1}; Y_{j,i}|W_1X_1^n) - I(Y_j^{i-1}; Y_{j,i}|W_1X_1^n) && (3.66)\\ &= \sum_{r=1}^{i-1}\Big[I(Y_j^{r-1}Z_r^{i-1}; Y_{j,i}|W_1X_1^n) - I(Y_j^rZ_{r+1}^{i-1}; Y_{j,i}|W_1X_1^n)\Big] && (3.67)\\ &= \sum_{r=1}^{i-1}\Big[I(Z_r; Y_{j,i}|Y_j^{r-1}Z_{r+1}^{i-1}W_1X_1^n) - I(Y_{j,r}; Y_{j,i}|Y_j^{r-1}Z_{r+1}^{i-1}W_1X_1^n)\Big] && (3.68)\\ &= \sum_{r=1}^{i-1}\Big[I(Z_r; Y_{j,i}|X_{1,r}Y_j^{r-1}Z_{r+1}^{i-1}W_1X_{1,r+1}^nX_1^{r-1}) - I(Y_{j,r}; Y_{j,i}|X_{1,r}Y_j^{r-1}Z_{r+1}^{i-1}W_1X_{1,r+1}^nX_1^{r-1})\Big] \\ &\overset{(a)}{\geq} 0 \ . && (3.69) \end{aligned}$$

The condition in (3.57) implies that for all $r \in [1 : i-1]$ and all V:

$$I(U; Y_r|VX_{1,r}) \leq I(U; Z_r|VX_{1,r}) \ . \tag{3.70}$$

Letting $U = Y_{j,i}$ and $V = Y_j^{r-1}Z_{r+1}^{i-1}W_1X_{1,r+1}^nX_1^{r-1}$, the claim in (a) is proved.

Thus,

$$nR_1 - n\,\epsilon_n \leq \sum_{i=1}^{n} I(W_1 X_1^n Y_j^{i-1}; Y_{j,i}) \tag{3.71}$$

$$\leq \sum_{i=1}^{n} I(W_1 X_1^n Z^{i-1}; Y_{j,i}) \ , \tag{3.72}$$

which completes the proof. □

Now that we have written an outer bound on the capacity region that is naturally extendable to the multicast CIFC, let us first define the very weak interference regime:

$$\forall P_{UX_1X_2} \ : \ \begin{cases} \forall j \in [1:N] \quad I(U;Y_j|X_1) \ \leq \ I(U;Z|X_1) \ , \\ \min\limits_{j\in[1:N]} I(UX_1;Y_j) \ \leq \ I(UX_1;Z) \ , \end{cases} \tag{3.73}$$

where $U \multimap (X_1, X_2) \multimap (Y_1, \cdots, Y_N, Z)$.

We can then state the following:

Theorem 30 (Very Weak Interference)**.** *The capacity region of the N-mutlicast CIFC in very weak interference regime is given by the set of rate pairs satisfying:*

$$\begin{cases} R_1 \ \leq \ \min\limits_{j\in[1:N]} I(X_1U;Y_j) \ , \\ R_2 \ \leq \ I(X_2;Z|X_1U) \ . \end{cases} \tag{3.74}$$

for some arbitrarily correlated (U, X_1, X_2) *satisfying* $U \multimap (X_1, X_2) \multimap (Y_1, \cdots, Y_N, Z)$.

Proof. The converse proof has been already stated. The achievability follows from the inner bound in (3.1) letting $Q = U$, $Q_1 = (X_1, U)$, and $V = X_2$. We end up with the inner bound:

$$\begin{cases} R_1 \ \leq \ \min\limits_{j\in[1:N]} I(X_1U;Y_j) \ , \\ R_2 \ \leq \ I(X_2;Z|X_1U) \ , \\ R_1 + R_2 \ \leq \ I(X_1X_2;Z) \ . \end{cases} \tag{3.75}$$

Using the very weak interference condition (3.73), the sum rate bound is redundant. Hence, the achievability is proved. □

3.5 Capacity region of the N-multicast CIFC in the mixed weak/strong interference regime

In this section, we consider a N-multicast CIFC where we can partition the multicast set of users into two subsets. A subset $\mathcal{W}$ where all users are in weak interference, and a subset $\mathcal{S}$ where users are in the strong interference regime, however, very weak or very strong interference can be verified in either of the sets, without being imposed on both sets. Hence, the two following holds for all $P_{UX_1X_2}$:

$$\forall j \in \mathcal{W} \quad , \quad I(U;Y_j|X_1) \leq I(U;Z|X_1) \ , \tag{3.76}$$

$$\forall j \in \mathcal{S} \quad , \quad I(X_2; Z|X_1) \leq I(X_2; Y_j|X_1) \ , \tag{3.77}$$

$$\min_{j\in\mathcal{S}} I(X_1X_2; Y_j) \leq I(X_1X_2; Z) \text{ Or } \min_{j\in\mathcal{W}} I(UX_1; Y_j) \leq I(UX_1; Z) \ . \tag{3.78}$$

The capacity region of this mixed very weak/strong interference setting can be deduced from the previous results on the strong/weak interference regimes, and can be obtained through a careful extension of the Interference Decoding principle.

Recall here that, in a multicast setting, ID allows of the users in the multicast group to decode/ or not the interference of the user Z, this will be crucial in the proof of achievability. As for the converse proof, it will rely only on the previously states arguments.

Theorem 31 (Mixed very weak/strong interference)**.** *The capacity region of the Multicast CIFC satisfying conditions* (3.76) –(3.78) *, is given by the set of rate pairs satisfying:*

$$\begin{cases} R_1 & \leq & \min\limits_{j\in\mathcal{W}} I(UX_1; Y_j) \ , \\ R_2 & \leq & I(X_2; Z|UX_1) \ , \\ R_1 + R_2 & \leq & \min\limits_{j\in\mathcal{S}} I(X_1X_2; Y_j) \ , \end{cases} \tag{3.79}$$

for some joint input pmf $P_{UX_1X_2}$ *satisfying* $U \multimap (X_1, X_2) \multimap (Y_1, \cdots, Y_N, Z)$ *.*

Proof. The converse proof follows in the exact same manner as the converse proof of both weak and strong interference cases. We can write thus:

$$nR_1 \leq \min_{j\in\mathcal{W}} \sum_{i=1}^{n} I(U_iX_{1,i}; Y_{j,i}) \ , \tag{3.80}$$

$$nR_2 \leq \sum_{i=1}^{n} I(X_{2,i}; Z_i|U_iX_{1,i}) \ , \tag{3.81}$$

$$n(R_1 + R_2) \leq \min_{j\in\mathcal{S}} \sum_{i=1}^{n} I(X_{1,i}X_{2,i}; Y_{j,i}) \ , \tag{3.82}$$

where $U_i = W_1X_{1,i+1}^nX_1^{i-1}Z^{i-1}$.

As for the achievability part, it is more involved and requires introducing the idea of interference decoding. The decoders Y_j with $j \in \mathcal{W}$ will choose to decode only the useful signal U and X_1 while the users that are in strong interference, i.e Y_j with $j \in \mathcal{S}$, will decode all signals transmitted by source 2 and source 1 : U X_1 and X_2.

Letting thus the codebook construction in D.1, and letting $Q_1 = \emptyset$, and $Q = U$ one could summarize the encoding constraints as follows:

$$T_1 - R_1 \geq I(U; X_1) \ , \tag{3.83}$$

$$T_2 - R_2 \geq I(V; X_1|U) \ . \tag{3.84}$$

As for the decoding constraints, user Z decodes the signal U and X_1 non uniquely, finding the unique s_2 such that for some w_1 and s_1

$$\left(u^n(s_1), x_1^n(w_1), v^n(s_1, s_2), y_j^n\right) \in T_\delta^n(UX_1VZ) \tag{3.85}$$

where $u^n(s_1)$ is in the bin defined by s_1. Thus, we end up with the constraints:

$$T_2 \leq I(V;Z|X_1U) + I(V;X_1|U) \ , \tag{3.86}$$

$$T_1 + T_2 \leq I(X_1UV;Z) + I(UV;X_1) \ . \tag{3.87}$$

On the other side, the users Y_j can choose between two decoding strategies:

- Not decoding interference, i.e finding the unique w_1 for which:

$$\left(u^n(s_1), x_1^n(w_1), y_j^n\right) \in T_\delta^n(UX_1Y_j) \ , \tag{3.88}$$

  where $u^n(s_1) \in B_1^n(w_1)$ is in the bin defined by w_1.

  This yields the following constraint:

$$T_1 \leq I(UX_1;Y_j) + I(U;X_1) \ . \tag{3.89}$$

- Decoding interference non uniquely, finding the unique w_1 such that for some s_2,

$$\left(u^n(s_1), x_1^n(w_1), v^n(s_1,s_2), y_j^n\right) \in T_\delta^n(UX_1VY_j) \ . \tag{3.90}$$

  This results in the constraint:

$$T_1 + T_2 \leq I(UX_1V;Y_j) + I(VU;X_1) \ . \tag{3.91}$$

One then can write an achievable inner bound with all possible combinations of decoding choices of each of the users Y_j.

In out setting, using this idea, we let the group of users in strong interference decode interference as well, and we let the users in weak interference decode only their intended signals U and X_1. The resulting set of constraints is given by:

$$\begin{cases} T_1 & \leq & \min\limits_{j\in\mathcal{W}} I(UX_1;Y_j) + I(U;X_1) \ , \\ T_2 & \leq & I(V;Z|X_1U) + I(V;X_1|U) \ , \\ T_1+T_2 & \leq & I(X_1UV;Z) + I(UV;X_1) \ , \\ T_1+T_2 & \leq & \min\limits_{j\in\mathcal{S}} I(UX_1V;Y_j) + I(UV;X_1) \ . \end{cases} \tag{3.92}$$

Running FME on the resulting rate region yields:

$$\begin{cases} R_1 & \leq & \min\limits_{j\in\mathcal{W}} I(UX_1;Y_j) \ , \\ R_2 & \leq & I(V;Z|X_1U) \ , \\ R_1+R_2 & \leq & I(X_1UV;Z) \ , \\ R_1+R_2 & \leq & \min\limits_{j\in\mathcal{S}} I(UX_1V;Y_j) \ . \end{cases} \tag{3.93}$$

Letting $V = X_2$, we end up with the following achievable region:

$$\begin{cases} R_1 & \leq & \min\limits_{j\in\mathcal{W}} I(UX_1;Y_j) \ , \\ R_2 & \leq & I(X_2;Z|X_1U) \ , \\ R_1+R_2 & \leq & I(X_1X_2;Z) \ , \\ R_1+R_2 & \leq & \min\limits_{j\in\mathcal{S}} I(X_1X_2;Y_j) \ . \end{cases} \tag{3.94}$$

with the strong interference or the weak interference condition, we can show that the sum-rate $R_1 + R_2 \leq I(X_1X_2;Z)$ is redundant.

This completes the proof of achievability. □

3.6 Comments on strong / weak interference

3.6.1 Anecdotic result

In a recent paper by Vaezi [49], it is shown that the " better cognitive decoding (BCD)" introduced in [26] is nothing but the mere "very weak interference (VWI)" regime and that the new capacity result in this regime is an equivalent formulation of the VWI capacity region. However, the astonishing result in the work of Vaezi lies in proving that the "very strong interference (VSI)" regime is contained in the VWI regime for finite alphabets suggesting that apparently contradictory regimes from a conceptual point of view, are in fact equivalent. Later on, we clarify how our work does not fall in such a triviality be it even for finite alphabet settings.

3.6.2 The multicast setting

A crucial remark here is that the claim of Vaezi that the class of probability distribution that verify "very strong interference(VSI)" falls into the class of "very weak interference(VWI)" or equivalently, the " better cognitive decoding (BCD)", this claim does not hold in the N-multicast setting.

Let us first review the claim of triviality of Vaezi. The three regimes are given by the following conditions:

$$\text{(VWI)}\ ,\ \forall P_{UX_1X_2} : \left\{ \begin{array}{rcl} I(U;Y|X_1) & \leq & I(U;Z|X_1) \\ I(X_1;Y) & \leq & I(X_1;Z) \end{array} \right. \tag{3.95}$$

$$\text{(BCD)}\ ,\ \forall P_{UX_1X_2} :\ I(UX_1;Y) \leq I(UX_1;Z) \tag{3.96}$$

$$\text{(VSI)}\ ,\ \forall P_{X_1X_2} : \left\{ \begin{array}{rcl} I(X_1X_2;Y) & \leq & I(X_1X_2;Z) \\ I(X_2;Z|X_1) & \leq & I(X_2;Y|X_1) \end{array} \right. \tag{3.97}$$

The key tool to show the equivalence between VWI and BCD is to notice that:

$$\forall P_{UX_1X_2}\ ,\ I(UX_1;Y) \leq I(UX_1;Z) \Rightarrow \forall P_{UX_1X_2}\ ,\ I(U;Y|X_1) \leq I(U;Z|X_1) \tag{3.98}$$

Thus, since:

$$I(X_1X_2;Y) \leq I(X_1X_2;Z) \text{ and } I(X_2;Z|X_1) \leq I(X_2;Y|X_1) \tag{3.99}$$

$$\Rightarrow \forall P_U\ ,\ I(UX_1;Y) \leq I(UX_1;Z)\ , \tag{3.100}$$

which means that VSI implies BCD which in turn is equivalent to VWI.

However, in our setting, the distinct regimes are defined by:

$$\text{(VWI)}\ ,\ \forall P_{UX_1X_2} : \left\{ \begin{array}{rcl} \forall j \in [1:N] \quad I(U;Y_j|X_1) & \leq & I(U;Z|X_1) \\ \min\limits_{j\in[1:N]} I(UX_1;Y) & \leq & I(UX_1;Z) \end{array} \right. \tag{3.101}$$

$$\text{(VSI)}\ ,\ \forall P_{X_1X_2} : \left\{ \begin{array}{rcl} \forall j \in [1:N] \quad I(X_2;Z|X_1) & \leq & I(X_2;Y_j|X_1) \\ \min\limits_{j\in[1:N]} I(X_1X_2;Y_j) & \leq & I(X_1X_2;Z) \end{array} \right. \tag{3.102}$$

It is clear when there is only one primary channel output, i.e $N = 1$, that what we recover is the BCD and the VSI regime. However, when $N > 1$, then, there is no evidence why the VSI should be included in the VWI since:

$$VSI \Rightarrow \min_{j\in[1:N]} I(UX_1; Y_j) \leq I(UX_1; Z) \tag{3.103}$$

but the other constraint of VWI can not be implied since it is too strict:

$$VSI \not\Rightarrow \forall j \in [1:N] \quad I(U; Y_j|X_1) \leq I(U; Z|X_1) \tag{3.104}$$

Thus, VSI can not imply VWI for all classes of multicast CIFC.

3.7 Capacity results for the Gaussian case

Consider the following Gaussian Multicast CIFC model as shown in Fig 3.1:

$$\forall j \in [1:N] \quad Y_j = b_j X_2 + X_1 + n_j \ , \tag{3.105}$$

$$Z = X_2 + aX_1 + n_z \ . \tag{3.106}$$

where b_j, $j \in [1:N]$, and a are real numbers, and where $n_1 \cdots n_N$, and n_z are additive white Gaussian noise components with powers $N_1 = \cdots = N_N = N_z = 1$.

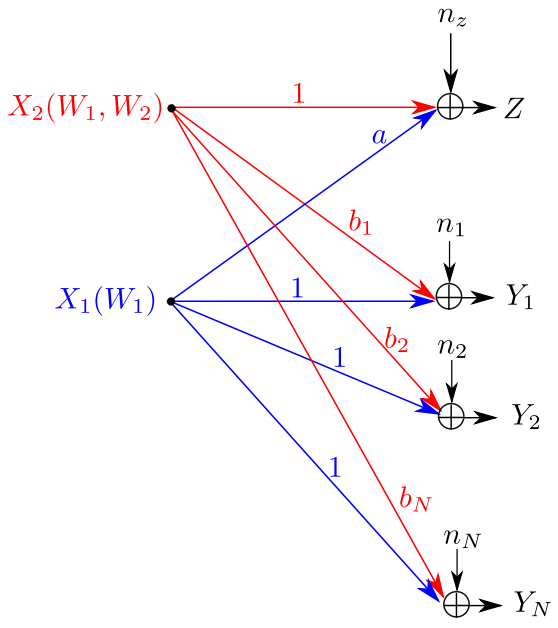


Figure 3.1: The Gaussian Multicast Cognitive Interference Channel

In this section, we derive the capacity region of many regimes in the Multicast Gaussian CIFC as listed below:

- The very strong interference regime

$$\left\{\begin{array}{rcl} \forall j \in [1:N] & , & |b_j| \geq 1 \ , \\ \forall \rho \in [-1:1] & , & \min\limits_{j\in[1:N]} \left\{ (1-a^2)P_1 + (b_j^2-1)P_2 + 2\rho(b_j-a)\sqrt{P_1P_2} \right\} \leq 0 \ . \end{array}\right. \tag{3.107}$$

- The weak interference

$$\forall j \in [1:N] \ , \ |b_j| \leq 1 \ . \tag{3.108}$$

- The mixed weak/very strong interference regime $[1:N] = \mathcal{S} \cup \mathcal{W}$ where:

$$\left\{\begin{array}{rcl} \forall j \in \mathcal{W} & , & |b_j| \leq 1 \ , \\ \forall j \in \mathcal{S} & , & |b_j| \geq 1 \ , \\ \forall \rho \in [-1:1] & , & \min\limits_{j\in\mathcal{S}} \left\{ (1-a^2)P_1 + (b_j^2-1)P_2 + 2\rho(b_j-a)\sqrt{P_1P_2} \right\} \leq 0 \ . \end{array}\right. \tag{3.109}$$

3.7.1 The very strong interference regime

The very strong interference regime is defined as follows:

$$\left\{\begin{array}{rcl} \forall j \in [1:N] & , & |b_j| \geq 1 \ , \\ \forall \rho \in [-1:1] & , & \min\limits_{j\in[1:N]} \left\{ (1-a^2)P_1 + (b_j^2-1)P_2 + 2\rho(b_j-a)\sqrt{P_1P_2} \right\} \leq 0 \ . \end{array}\right. \tag{3.110}$$

Theorem 32. *The capacity region in the very strong interference regime consists in the set of rate pairs satisfying:*

$$\left\{\begin{array}{rcl} R_2 & \leq & \frac{1}{2}\log_2\left(1+(1-\rho^2)P_2\right) \ , \\ R_1+R_2 & \leq & \frac{1}{2}\min\limits_{j\in[1:N]} \log_2\left(1+b_j^2P_2+P_1+2b_j\rho\sqrt{P_1P_2}\right) \ . \end{array}\right. \tag{3.111}$$

for some $\rho \in [-1:1]$.

Proof. We start with the achievability part. Consider the following coding scheme:

$$(X_1,X_2) \sim \mathcal{N}\left(\mathbf{0}, \left[\begin{array}{cc} P_1 & \rho\sqrt{P_1P_2} \\ \rho\sqrt{P_1P_2} & P_2 \end{array}\right]\right) \ . \tag{3.112}$$

Then, letting $j \in [1:N]$:

$$I(X_1X_2;Y_j) = \frac{1}{2}\log_2\left(1+b_j^2P_2+P_1+2b_j\rho\sqrt{P_1P_2}\right) \ , \tag{3.113}$$

$$I(X_2;Z|X_1) = \frac{1}{2}\log_2\left(1+(1-\rho^2)P_2\right) \ . \tag{3.114}$$

which completes the proof of achievability.

As for the converse, following the same lines as the proof of the outer bound in section 3.2, we can write the following outer bound as:

$$\left\{\begin{array}{rcl} R_1 & \leq & \min\limits_{j\in[1:N]} I(X_1X_2;Y_j)\ , \\ R_2 & \leq & I(X_2;Z|X_1)\ , \\ R_1+R_2 & \leq & \min\limits_{j\in[1:N]} I(X_1X_2;Y_j)+I(X_2;Z|Y_j'X_1)\ . \end{array}\right. \tag{3.115}$$

Similarly to the result of Rini *et.al* [45], we compute the optimal correlation coefficient between$Z$ and Y_j' conditioned on X_1. We obtain then, the following outer bound:

$$\left\{\begin{array}{rcl} R_2 & \leq & \frac{1}{2}\log_2\left(1+(1-\rho^2)P_2\right)\ , \\ R_1 & \leq & \frac{1}{2}\min\limits_{j\in[1:N]}\log_2\left(1+b_j^2P_2+P_1+2b_j\rho\sqrt{P_1P_2}\right)\ , \\ R_1+R_2 & \leq & \frac{1}{2}\min\limits_{j\in[1:N]}\left[\log_2\left(1+b_j^2P_2+P_1+2b_j\rho\sqrt{P_1P_2}\right)+\frac{1}{2}\log_2^+\left(\frac{1+(1-\rho^2)P_2}{1+(1-\rho^2)P_2b_j^2}\right)\right]\ . \end{array}\right. \tag{3.116}$$

where $\log_2^+(x)\triangleq\max(0,\log_2(x))$.

Since $|b_j|>1$ for all $j\in[1:N]$, then the outer bound becomes equal to:

$$\left\{\begin{array}{rcl} R_2 & \leq & \frac{1}{2}\log_2\left(1+(1-\rho^2)P_2\right)\ , \\ R_1+R_2 & \leq & \frac{1}{2}\min\limits_{j\in[1:N]}\log_2\left(1+b_j^2P_2+P_1+2b_j\rho\sqrt{P_1P_2}\right)\ . \end{array}\right. \tag{3.117}$$

which proves our claim. □

3.7.2 The weak interference regime

Assume that :

$$\forall j\in[1:N]\ ,\quad |b_j|<1\ . \tag{3.118}$$

Though this condition is looser that the very weak interference regime, we are able to recover the capacity region in the Gaussian case restricting only to weak interference regime.

Then, one important claim is that, conditioned on X_1, all Y_j are degraded versions of Z given X_1; this will be crucial in the proof of converse.

Theorem 33. *The capacity region in the weak interference regime is given by the set of rate pairs satisfying:*

$$\left\{\begin{array}{rcl} R_1 & \leq & \frac{1}{2}\max\limits_{\rho\in[-1:1]}\min\limits_{j\in[1:N]}\log_2\left(\frac{1+b_j^2P_2+P_1+2b_j\rho\sqrt{(1-\alpha)P_1P_2}}{1+b_j^2\alpha P_2}\right)\ , \\ R_2 & \leq & \frac{1}{2}\log_2\left(1+\alpha P_2\right)\ . \end{array}\right. \tag{3.119}$$

for some $\alpha\in[0:1]$.

Proof. The achieavability follows from the achievable rate region:

$$\left\{ \begin{array}{rcl} R_1 & \leq & \min\limits_{j\in[1:N]} I(X_1U;Y_j) \ , \\ R_2 & \leq & I(V;Z) - I(V;X_1U) \ . \end{array} \right. \tag{3.120}$$

obtained through the inner bound (3.1) letting $Q_1 = Q = \emptyset$ and considering only one of the resulting corner points.

The optimal coding scheme is then to let:

$$X_2 = X_u + X_v \quad , \quad X_v \sim \mathcal{N}(0, \alpha P_2) \quad , \quad X_u \sim \mathcal{N}(0, (1-\alpha)P_2) \ , \tag{3.121}$$

$$U = X_u \quad , \quad X_1 \sim \mathcal{N}(0, P_1) \ , \tag{3.122}$$

$$(X_1, X_u) \sim \mathcal{N}\left(\mathbf{0}, \left[\begin{array}{cc} P_1 & \rho\sqrt{P_1(1-\alpha)P_2} \\ \rho\sqrt{P_1(1-\alpha)P_2} & (1-\alpha)P_2 \end{array} \right]\right) \ , \tag{3.123}$$

$$V = X_v + \gamma(X_u + aX_1) \ , \tag{3.124}$$

where $|\rho| \leq 1$ and γ is the optimal Dirty Paper Coding parameter to precode against the interference $X_u + aX_1$ seen at user Z.

Thus, we obtain:

$$I(X_uX_1;Y_j) = h(Y_j) - h(Y_j|X_uX_1) \tag{3.125}$$

$$= \frac{1}{2}\log_2\left(\frac{1 + b_j^2P_2 + P_1 + 2b_j\rho\sqrt{(1-\alpha)P_1P_2}}{1 + b_j^2\alpha P_2}\right) \ , \tag{3.126}$$

and

$$I(V;Z) - I(V;UX_1) = I(X_v;Z|X_1X_u) = \frac{1}{2}\log_2(1+\alpha P_2) \ . \tag{3.127}$$

N.B: It is because we can apply DPC techniques for the Gaussian case that we are able to relax the constraint of very weak interference to only weak interference. In the general case, it is not possible for user Z to decode interference unless its resulting sum rate is satisfied, i.e $R_1 + R_2 \leq I(X_1X_2;Z)$.

The parameter ρ can not be optimized for each instance of the primary channels Y_j since the b_js are not all compulsorily equal (in sign and module), leading us to the max min expression.

Hereafter, the converse proof. Let us start by writing

$$nR_2 = H(W_2) \tag{3.128}$$

$$\overset{(a)}{\leq} I(W_2;Z^n) + n\epsilon_n \tag{3.129}$$

$$\overset{(b)}{\leq} I(W_2;Z^n|W_1X_1^n) + n\epsilon_n \tag{3.130}$$

$$\overset{(c)}{\leq} I(X_2^n;Z^n|W_1X_1^n) + n\epsilon_n \ , \tag{3.131}$$

where (a) is a consequence of Fano's inequality and (b) follows from the fact that W_2 is independent of both W_1 and X_1^n, and (c) results from the fact that the following Markov Chain holds $W_2 \multimap (X_2^n, X_1^n, W_1) \multimap Z^n$.

Then, let $j \in [1:N]$; we have that:

$$\begin{aligned} nR_1 &= H(W_1) && (3.132)\\ &\leq I(W_1;Y_j^n) + n\epsilon_n && (3.133)\\ &\leq I(W_1X_1^n;Y_j^n) + n\epsilon_n \ , && (3.134)\end{aligned}$$

Next, we bound the two resulting rates.
Since,

$$\frac{n}{2}\log_2(2\pi e) \leq h(Z^n|W_1X_1^n) \leq \frac{n}{2}\log_2(P_2+1) + \frac{n}{2}\log_2(2\pi e) \ . \quad (3.135)$$

Thus,

$$\exists \alpha \in [0:1] \quad \text{s.t,} \quad h(Z^n|W_1X_1^n) = \frac{n}{2}\log_2(\alpha P_2+1) + \frac{n}{2}\log_2(2\pi e) \ , \quad (3.136)$$

and since,

$$h(Z^n|X_2^nX_1^n) = \frac{n}{2}\log_2(2\pi e) \ , \quad (3.137)$$

we can conclude that

$$R_2 \leq \frac{1}{n}I(X_2^n;Z^n|W_1X_1^n) = \frac{1}{2}\log_2(\alpha P_2+1) \ . \quad (3.138)$$

Next, note that, with an abuse of notations:

$$Y_j^n|X_1^n = b_jX_2^n + n_2^n = b_j(Z^n|X_1^n) + b_j\tilde{n}_2^n \ , \quad (3.139)$$

where $\tilde{n}_2 \sim \mathcal{N}(0, \frac{1}{b_j^2}-1)$.

Thus, we can write by the n-letter conditional EPI that:

$$\begin{aligned} h(Y_j^n|W_1X_1^n) &\geq \frac{n}{2}\log_2\left(2^{\frac{2}{n}h(b_jZ^n|W_1X_1^n)} + 2^{\frac{2}{n}h(b_j\tilde{n}_2^n)}\right) && (3.140)\\ &= \frac{n}{2}\log_2\left(b_j^2 2^{\frac{2}{n}h(Z^n|W_1X_1^n)} + 2\pi e(1-b_j^2)\right) && (3.141)\\ &= \frac{n}{2}\log_2\left(b_j^2(\alpha P_2+1) + 1 - b_j^2\right) + \frac{n}{2}\log_2(2\pi e) && (3.142)\\ &= \frac{n}{2}\log_2\left(b_j^2\alpha P_2 + 1\right) + \frac{n}{2}\log_2(2\pi e) \ , && (3.143)\end{aligned}$$

Plus, letting besides (X_1, X_2) with the following covariance matrix:

$$K = \begin{bmatrix} P_1 & \rho_{12}\sqrt{P_1P_2} \\ \rho_{12}\sqrt{P_1P_2} & P_2 \end{bmatrix} \ , \quad (3.144)$$

we can combine with:

$$\frac{n}{2}\log_2\left(2\pi e(b_j^2\alpha P_2+1)\right) \leq h(Y_j^n|W_1X_1^n) \leq h(Y_j^n|X_1^n) \leq \frac{n}{2}\log_2(2\pi e(b_j^2(1-\rho_{12}^2)P_2+1)) \ , \quad (3.145)$$

thus,

$$\alpha \leq 1-\rho_{12}^2 \ . \quad (3.146)$$

Thus, we let: $\rho \in [-1:1]$ such that

$$\rho = \frac{\rho_{12}}{\sqrt{1-\alpha}} \ , \tag{3.147}$$

Finally, we obtain:

$$R_1 \leq \frac{1}{2}\log_2\left(1 + b_j^2\alpha P_2 + P_1 + 2b_j\rho\sqrt{P_1(1-\alpha)P_2}\right) - \frac{1}{2}\log_2\left(b_j^2\alpha P_2 + 1\right) \ , \tag{3.148}$$

which ends our proof. □

3.7.3 The mixed weak/very strong interference regime

We define the mixed weak/very strong interference regime by a partition $[1:N] \triangleq \mathcal{S} \cup \mathcal{W}$ where:

$$\left\{\begin{array}{rcl} \forall j \in \mathcal{S} & , & |b_j| \geq 1 \ , \\ \forall j \in \mathcal{W} & , & |b_j| \leq 1 \ , \\ \forall \rho \in [-1:1] & , & \min\limits_{j\in\mathcal{S}}\left\{(1-a^2)P_1 + (b_j^2-1)P_2 + 2\rho(b_j-a)\sqrt{P_1P_2}\right\} \leq 0 \ . \end{array}\right. \tag{3.149}$$

The capacity region of this setting is given by the following result.

Theorem 34. *The capacity region of the mixed weak/very strong interference regime is given by the set of rate pairs that satisfy:*

$$\left\{\begin{array}{rcl} R_1 & \leq & \frac{1}{2}\min\limits_{j\in\mathcal{W}}\log_2\left(\frac{1 + b_j^2P_2 + P_1 + 2b_j\rho\sqrt{(1-\alpha)P_1P_2}}{1+b_j^2\alpha P_2}\right) \ , \\ R_2 & \leq & \frac{1}{2}\log_2\left(1+\alpha P_2\right) \ , \\ R_1+R_2 & \leq & \frac{1}{2}\min\limits_{j\in\mathcal{S}}\log_2\left(1 + b_j^2P_2 + P_1 + 2b_j\rho\sqrt{(1-\alpha)P_1P_2}\right) \ , \end{array}\right. \tag{3.150}$$

for some $\alpha \in [0:1]$ *and* $\rho \in [-1:1]$.

Proof. Achievability follows from evaluating the rate region given by:

$$\left\{\begin{array}{rcl} R_1 & \leq & \min\limits_{j\in\mathcal{W}} I(UX_1;Y_j) \ , \\ R_2 & \leq & I(X_2;Z|UX_1) \ , \\ R_1+R_2 & \leq & \min\limits_{j\in\mathcal{S}} I(X_1X_2;Y_j) \ , \end{array}\right. \tag{3.151}$$

with the following coding scheme:

$$X_2 = X_u + X_v \quad , \quad X_v \sim \mathcal{N}(0,\alpha P_2) \quad , \quad X_u \sim \mathcal{N}(0,(1-\alpha)P_2) \ , \tag{3.152}$$

$$U = X_u \quad , \quad X_1 \sim \mathcal{N}(0,P_1) \ , \tag{3.153}$$

$$(X_1,X_u) \sim \mathcal{N}\left(\mathbf{0}, \left[\begin{array}{cc} P_1 & \rho\sqrt{P_1(1-\alpha)P_2} \\ \rho\sqrt{P_1(1-\alpha)P_2} & (1-\alpha)P_2 \end{array}\right]\right) \ , \tag{3.154}$$

where $|\rho| \leq 1$. Then we obtain:

$$I(X_u X_1; Y_j) = h(Y_j) - h(Y_j|X_u X_1) \tag{3.155}$$

$$= \frac{1}{2}\log_2\left(\frac{1 + b_j^2 P_2 + P_1 + 2b_j\rho\sqrt{(1-\alpha)P_1 P_2}}{1 + b_j^2\alpha P_2}\right) , \tag{3.156}$$

and

$$I(X_2; Z|X_1 X_u) = \frac{1}{2}\log_2\left(1 + \alpha P_2\right) , \tag{3.157}$$

and finally:

$$I(X_2 X_1; Y_j) = \frac{1}{2}\log_2\left(1 + b_j^2 P_2 + P_1 + 2b_j\rho\sqrt{(1-\alpha)P_1 P_2}\right) . \tag{3.158}$$

As for the outer bound, we can, similarly to the weak and strong interference case, write that:

$$nR_1 \leq \min_{j\in\mathcal{W}} I(W_1 X_1^n; Y_j^n) + n\epsilon_n , \tag{3.159}$$

$$nR_2 \leq I(X_2^n; Z^n|W_1 X_1^n) + n\epsilon_n , \tag{3.160}$$

$$n(R_1 + R_2) \leq \min_{j\in\mathcal{S}} I(X_1^n X_2^n; Y_j^n) + n\epsilon_n . \tag{3.161}$$

In the same fashion again, define $\alpha \in [0:1]$ such that:

$$h(Z^n|W_1 X_1^n) = \frac{n}{2}\log_2(\alpha P_2 + 1) + \frac{n}{2}\log_2(2\pi e) \tag{3.162}$$

We can show that for all $j \in \mathcal{W}$,

$$h(Y_j^n|W_1 X_1^n) \geq \frac{n}{2}\log_2(\alpha b_j^2 P_2 + 1) + \frac{n}{2}\log_2(2\pi e) . \tag{3.163}$$

As for $h(Y_j^n)$ with $j \in [1:N]$, it is maximized with (X_1, X_2) jointly Gaussian with the covariance matrix:

$$K = \begin{bmatrix} P_1 & \rho_{12}\sqrt{P_1 P_2} \\ \rho_{12}\sqrt{P_1 P_2} & P_2 \end{bmatrix} , \tag{3.164}$$

where $\rho_{12} \in [-1:1]$.

Now, it can be noticed that ρ_{12} has to satisfy the inequality:

$$\alpha \leq 1 - \rho_{12}^2 . \tag{3.165}$$

Thus, we let: $\rho \in [-1:1]$ such that

$$\rho = \frac{\rho_{12}}{\sqrt{1-\alpha}} , \tag{3.166}$$

and end up with an outer bound equal to the claimed capacity region (3.150). □

3.7.4 Special cases

In the sequel we give a more compact expression of the capacity region for the weak interference regime.

Corollary 1) If all $b_j s$ are of the same sign, i.e coherent weak interference, then, the capacity region in weak interference is given by the set of rate pairs satisfying:

$$\mathcal{C}_{WI}(\alpha) \ : \ \begin{cases} R_1 & \leq & \frac{1}{2} \min\limits_{j\in[1:N]} \log_2 \left(\frac{1+b_j^2 P_2 + P_1 + 2|b_j|\sqrt{(1-\alpha)P_1 P_2}}{1+b_j^2 \alpha P_2} \right) \ , \\ R_2 & \leq & \frac{1}{2}\log_2\left(1+\alpha P_2\right) \ . \end{cases} \tag{3.167}$$

Moreover, the capacity region consists of the intersection of all capacity regions of the CIFCs $(Z;Y_j)$.

2) If all $b_j s$ are of the same sign, i.e coherent strong interference, then, the capacity region is given by the set of rate pairs satisfying:

$$\mathcal{C}_{SI}(\alpha) \ : \ \begin{cases} R_2 & \leq & \frac{1}{2}\log_2\left(1+\alpha P_2\right) \ , \\ R_1+R_2 & \leq & \frac{1}{2} \log_2\left(1+b_*^2 P_2 + P_1 + 2|b_*|\sqrt{P_1 P_2}\right) \ , \end{cases} \tag{3.168}$$

where

$$|b_*| \triangleq \min_{j\in[1:N]} |b_j| \ . \tag{3.169}$$

Moreover, the capacity region consists of the intersection of all capacity regions of the CIFCs $(Z;Y_j)$

3) If all b_js are of the same sign, coherent mixed interference, then the capacity region is given by the set of rate pairs satisfying:

$$\begin{cases} R_1 & \leq & \frac{1}{2} \min\limits_{j\in\mathcal{W}} \log_2 \left(\frac{1+b_j^2 P_2 + P_1 + 2|b_j|\sqrt{(1-\alpha)P_1 P_2}}{1+b_j^2 \alpha P_2} \right) \ , \\ R_2 & \leq & \frac{1}{2}\log_2\left(1+\alpha P_2\right) \ , \\ R_1+R_2 & \leq & \frac{1}{2} \min\limits_{j\in\mathcal{S}} \log_2\left(1+b_j^2 P_2 + P_1 + 2|b_j|\sqrt{(1-\alpha)P_1 P_2}\right) \ . \end{cases} \tag{3.170}$$

Plus, the capacity region is given by the intersection of the single capacity regions.

Proof. The three claims have similar proofs. We only show the first claim.

The first part of the proof is trivial, since the optimal ρ is obtained by $+1$ if all channel coefficients b_j are positive, and -1 otherwise.

The second half of the claim can be proved defining the following. Let C_j be the capacity region of the CIFC (Z, Y_j) in weak interference. Assume wolog that all b_js are positive. We have that:

$$\mathcal{C}_j(\alpha) \ : \ \begin{cases} R_1 & \leq & R_{1,j}(\alpha) \triangleq \frac{1}{2} \log_2 \left(\frac{1+b_j^2 P_2 + P_1 + 2b_j\sqrt{(1-\alpha)P_1 P_2}}{1+b_j^2 \alpha P_2} \right) \ , \\ R_2 & \leq & R_2(\alpha) \triangleq \frac{1}{2}\log_2\left(1+\alpha P_2\right) \ . \end{cases} \tag{3.171}$$

We want to show that:

$$\bigcap_{j=1}^{N} \bigcup_{\alpha} \mathcal{C}_j(\alpha) = \bigcup_{\alpha} \mathcal{C}(\alpha) \ . \tag{3.172}$$

We have that for all $j \in [1:N]$, $\mathcal{C}(\alpha) \subset \mathcal{C}_j(\alpha)$, thus it is easy to prove the first inclusion

$$\bigcup_{\alpha} \mathcal{C}(\alpha) \subset \bigcap_{j=1}^{N} \bigcup_{\alpha} \mathcal{C}_j(\alpha) \ . \tag{3.173}$$

Now, to show the other inclusion, let (R_1, R_2) be a rate pair in $\subset \bigcap_{j=1}^{N} \bigcup_{\alpha} \mathcal{C}_j(\alpha)$, we want to show that (R_1, R_2) lies in $\bigcup_{\alpha} \mathcal{C}(\alpha)$.

Let $\alpha_1 ... \alpha_N$ be N parameters such that:

$$\begin{cases} R_1 & \leq & \min\limits_{j\in[1:N]} R_{1,j}(\alpha_j) \ , \\ R_2 & \leq & \min\limits_{j\in[1:N]} R_2(\alpha_j) \ . \end{cases} \tag{3.174}$$

Note that, R_2 is increasing in α while $R_{1,j}$ is decreasing in α. Thus, we have

$$R_2 \leq \min_{j\in[1:N]} R_2(\alpha_j) = R_2(\min_{j\in[1:N]} \alpha_j) \ . \tag{3.175}$$

And hence, since $R_{1,j}$ is decreasing in α, then:

$$R_1 \leq \min_{j\in[1:N]} R_{1,j}(\alpha_j) \leq \min_{j\in[1:N]} R_{1,j}(\min_{j\in[1:N]} \alpha_j) \ , \tag{3.176}$$

thus, defining $\alpha = \min\limits_{j\in[1:N]} \alpha_j$ allows (R_1, R_2) to lie in the region $\bigcup_{\alpha} \mathcal{C}(\alpha)$. □

Summary

In this second part of the thesis, we studied the Multicast Cognitive Interference Channel or equivalently the Broadcast Channel with a helper and a common message. The focus was on the characterization of many interference regimes based on known results for the Cognitive Interference Channel.

In the overall very strong interference regime, when all users experience strong interference, we were able to show that the straightforward extension of the optimal scheme to the Multicast case is capacity achieving.

As for the overall weak interference regime, the extension is not straightforward since the outer bounding technique known to date relies on the use of Csiszár & Körner's sum identity, which has long remained impossible to extend to multiple user outputs. Thus, we had to rewrite a novel outer bound without resorting to this sum identity, and based on the obtained result, a straightforward extension to the multiple users case was possible.

As a more challenging regime, when each user among the multicast set of users experiences each either weak or strong interference, the combination of both optimal schemes in weak and strong interference allowed us to recover the capacity region of such a mixed regime.

Last, we characterized the capacity regions of the corresponding Gaussian cases resorting to standard Gaussian signalling and upper bounding techniques. An important output of this part of the work is the distinction between the coherent and non coherent interference regime. In the coherent interference regime, the capacity region is yielded by the intersection of all single capacity regions formed by the secondary user and each of the primary users. When interference is not coherent, then a bigger impediment is engendered by the fact that a tradeoff is imposed by the opposite signalling directions.

Part III

The Wiretap Broadcast Channel

Introduction and Setup

1 Introduction

Information theoretic secrecy was first introduced by Shannon in his seminal work [9] where he investigates a communication system between a source, a *legitimate* receiver and an *eavesdropper* where the source and the legitimate receiver share a secret key. It is shown that, to achieve perfect secrecy, one has to let the key rate be at least as large as the message rate. This result motivated the work [2] by Wyner who introduced the notion of Wiretap Channel. In such a setting, a source wishes to transmit a message to a *legitimate* receiver in the presence of an *eavesdropper* but without resorting to a shared key. Besides communicating reliably to the legitimate receiver at a maximum rate, the source has to maximize the equivocation at the eavesdropper so that it cannot recover the message sent over the channel. In the case of perfect secrecy, the conditional probability of the message given the eavesdropper's observation has to be approximately uniform over the set of messages, i.e., there is no leakage of information to the eavesdropper. The surprising result of Wyner's work [2] is that the use of a secret key is no longer required to guarantee a positive equivocation rate or even perfect secrecy. Csiszár & Körner's [21] generalized this result –first derived with the assumption of a degraded eavesdropper– to the general BC and where the source must also transmit a common message to both users. As a matter of fact, an analysis of the corresponding rate region regarding the necessity of two auxiliary random variables, namely, rate splitting and channel prefixing, was carried out by Ozel & Ulukus in [50]. It was shown that under specific channel ordering the rate region requires only one or even none of these variables.

Several multi-terminal Wiretap networks were studied, e.g., the MAC Wiretap Channel has been investigated by Liang & Poor in [51] while physical layer security in broadcast networks was studied by Liang *et al.* in [52] though, the capacity region is yet to be fully characterized.

Related works

The Wiretap Broadcast Channel (WBC) was first studied under two types of secrecy constraints.

The Broadcast Channel with confidential messages where the encoder transmits two private messages, each to its respective user, while keeping both of them secret from the opposite user. In [53], inner and outer bounds on the secrecy capacity were derived. The secrecy capacity of the semi-deterministic BC with confidential messages is derived in [54]

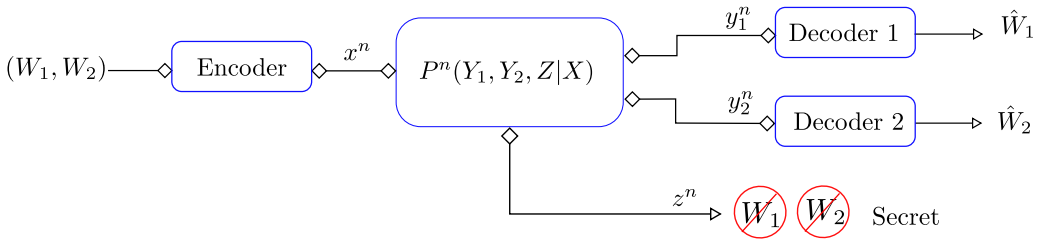


Figure 1: The Wiretap Broadcast Channel.

while in [55] it is assumed that only one message has to be kept secret from the other user and the capacity of the semi-deterministic eavesdropper setting was characterized. As for the Gaussian MIMO BCs with confidential messages, it was considered in the works of Liu *et al.* in [56, 57] while the Gaussian MIMO multi-receiver wiretap channel was addressed by Ekrem & Ulukus in [58] (see [59, 60] and references therein).

An alternate setting is the BC with an *external eavesdropper* where the secrecy requirement consists in that all messages be kept secret from the eavesdropper which is different from both users. Following this setting, the capacity of some classes of ordered and product BCs were first investigated by Ekrem & Ulukus in [22], where the legitimate users' channels exhibit a degradedness order and the eavesdropper is *more-noisy* than all legitimate users' channels. In a concurrent work by Bagherikaram *et al.* in [23], the secrecy capacity was characterized for the case where the eavesdropper is *degraded* towards the weakest user and also for its corresponding additive white Gaussian noise (AWGN) channel model.

Main contributions

In this work, we consider the Wiretap BC where the encoder transmits two private messages to two users while it wishes to keep them secret from an external eavesdropper. We derive both an outer bound and an inner bound on the secrecy capacity region of this setting. The outer bound is obtained through a careful single-letter derivation that addresses the main difficulty of our setting which relies on upper bounding techniques for three terminals' problems. It should be emphasized that both converse techniques for the standard BC and the Wiretap Channel require the use of Csiszár & Körner's sum-identity [21] which does not apply to more than two output sequences. Besides this well-known difficulty, our outer bound clearly copies the mathematical form and behaviour of the best known outer bound for the BC without an eavesdropper [28]. As for the inner bound, our techniques simply follow the notion of *double binning*, *superposition coding* and *bit recombination*. Moreover, in the absence of secrecy requirement, the obtained inner bound naturally reduces to Marton's inner bound for the BC with common message [3].

By developing an equivalent but non-straightforward representation of the outer bound, we show that it matches the inner bound for several novel classes of non-degraded Wiretap Broadcast Channels. More precisely, we are able to characterize the secrecy region of the following settings:

1. The deterministic BC with an arbitrary eavesdropper where both legitimate users

observe a deterministic function of the input,

2. The semi-deterministic BC with a more-noisy eavesdropper where only one of the legitimate users is a deterministic channel while the other is less-noisy than the eavesdropper,

3. The less-noisy BC with an eavesdropper degraded respect to the best legitimate user,

4. The product of two inversely less-noisy BC with a more-noisy eavesdropper.

Besides novel secrecy capacity results, the outer and inner bounds also recover some known results, e.g., the degraded BC with a more-noisy eavesdropper [22] which generalizes the degraded BC with a degraded eavesdropper [23].

We finally illustrate the results by investigating the impact of secrecy constraints on the capacity of the Wiretap Broadcast Channel with binary erasure (BEC) and binary symmetric (BSC) components. To his end, we derive the secrecy capacity region of a Less Noisy BEC/BSC BC with a degraded BSC eavesdropper and compare it to the standard capacity region, i.e. without secrecy constraints. In this setting, the central difficulty arises from the converse part for which we were able to show, through convexity arguments, a novel inequality on the conditional entropy of binary sequences. Indeed, this inequality appears to be crucial in the study of the WBC with BSC and BEC components, similar to Mrs. Gerber's lemma [61] for the binary symmetric BC. The analysis of the secrecy capacity region proved that the degraded eavesdropper's impediment can be very severe on the BSC user whilst, it would still allow, for the worst degraded case, for positive rates for the BEC user.

2 Problem Definition

Hereafter, we introduce the Wiretap Broadcast Channel as represented in Fig. 1, and then derive both an outer and an inner bound on its secrecy capacity region.

- Consider an n-th extension of a three-user memoryless Broadcast Channel:

$$\mathcal{W}^n = \left\{ P_{Y_1^n Y_2^n Z^n|X^n} : \mathcal{X}^n \longmapsto \mathcal{Y}_1^n \times \mathcal{Y}_2^n \times \mathcal{Z}^n \right\}, \tag{1}$$

  defined by the conditional p.m.f:

$$P_{Y_1^n Y_2^n Z^n|X^n} \triangleq \prod_{i=1}^{n} P_{Y_{1,i} Y_{2,i} Z_i|X_i} \ . \tag{2}$$

- An (M_{1n}, M_{2n}, n)-code for this channel consists of: two sets of messages $\mathcal{M}_1$ and $\mathcal{M}_2$, an encoding function that assigns an n-sequence $x^n(w_1, w_2)$ to each message pair $(w_1, w_2) \in \mathcal{M}_1 \otimes \mathcal{M}_1$ and decoding functions, one at each receiver, that assign to the received signal an estimate message $(\hat{w}_j)$ in $\mathcal{M}_j, j \in \{1, 2\}$ or an error.
  The probability of error is given by:

$$P_e^{(n)} \triangleq \mathbb{P}\left(\bigcup_{j \in \{1,2\}} \left\{ \hat{W}_j \neq W_j \right\} \right). \tag{3}$$

- A rate pair (R_1, R_2) is said to be achievable if there exists an (M_{1n}, M_{2n}, n)-code satisfying:

$$\liminf_{n\to\infty} \frac{1}{n} \log_2 M_{jn} \geq R_j \quad \forall\, j \in \{1,2\}\,, \tag{4}$$

$$\limsup_{n\to\infty} P_e^{(n)} = 0\ , \tag{5}$$

$$\liminf_{n\to\infty} \frac{1}{n} H(W_1 W_2 | Z^n) \geq R_1 + R_2\ . \tag{6}$$

  Note that the last constraint implies that for some sequence ϵ_n of positive values:

$$I(W_1 W_2; Z^n) \leq n\epsilon_n\ , \tag{7}$$

  which implies individual secrecy constraints given by

$$I(W_j; Z^n) \leq n\epsilon_n\ ,\ \forall\, j \in \{1,2\}. \tag{8}$$

- The secrecy capacity region is the closure of the set of all achievable rate pairs (R_1, R_2).

Chapter 4

On the secrecy capacity region of the Wiretap BC

In this part of the thesis, we derive both an outer and an inner bound on the secrecy capacity region of the Wiretap BC. Later, we show that these bounds are tight for some classes of Wiretap BCs and evaluate a numerical example consisting in a BEC/BSC BC with a BSC eavesdropper.

4.1 Main Results

4.1.1 Outer bound on the secrecy capacity region of the Wiretap BC

We next present an outer bound on the secrecy capacity region of the WBC under study. This bound originates from a careful single-letter characterization and accounts for different channel configurations which provides the secrecy capacity region for some new classes of wiretap broadcast channels.

Theorem 35 (Outer bound)**.** *The secrecy capacity region of the Wiretap BC with an external eavesdropper is included in the set of rate pairs satisfying:*

$$R_1 \leq I(U_1;Y_1|TV_1) - I(U_1;Z|TV_1) \ , \tag{4.1}$$
$$R_1 \leq I(U_1;Y_1Y_2|TV_1V_2) - I(U_1;Z|TV_1V_2) \ , \tag{4.2}$$
$$R_1 \leq I(U_1;Y_1|TV_1U_2) - I(U_1;Z|TV_1U_2) \ , \tag{4.3}$$
$$R_1 \leq I(U_1;Y_1Y_2|TV_1U_2V_2) - I(U_1;Z|TV_1U_2V_2) \ , \tag{4.4}$$
$$R_2 \leq I(U_2;Y_2|TV_2) - I(U_2;Z|TV_2) \ , \tag{4.5}$$
$$R_2 \leq I(U_2;Y_2Y_1|TV_1V_2) - I(U_2;Z|TV_1V_2) \ , \tag{4.6}$$
$$R_2 \leq I(U_2;Y_2|TV_2U_1) - I(U_2;Z|TV_2U_1) \ , \tag{4.7}$$
$$R_2 \leq I(U_2;Y_2Y_1|TU_1V_1V_2) - I(U_2;Z|TU_1V_1V_2) \ , \tag{4.8}$$
$$R_1 + R_2 \leq I(X;Y_2|TZV_1) + I(U_1S_1;Y_1|TV_1) - I(U_1S_1;ZY_2|TV_1) \ , \tag{4.9}$$
$$R_1 + R_2 \leq I(X;Y_2|TZV_1V_2) + I(U_1S_1;Y_1Y_2|TV_1V_2) - I(U_1S_1;ZY_2|TV_1V_2) \ , \tag{4.10}$$

$$R_1 + R_2 \leq I(X;Y_1|TZV_2) + I(U_2S_2;Y_2|TV_2) - I(U_2S_2;ZY_1|TV_2) \ , \quad (4.11)$$
$$R_1 + R_2 \leq I(X;Y_1|TZV_1V_2) + I(U_2S_2;Y_2Y_1|TV_1V_2) - I(U_2S_2;ZY_1|TV_1V_2) \ , \quad (4.12)$$

for some joint input p.m.f $P_{TV_1V_2U_1U_2S_1S_2X} = P_{TV_1V_2U_1U_2S_1S_2}P_{X|U_1U_2S_1S_2}$.

Proof: The proof of this theorem is relegated to Section 4.4. ■

The next corollary proceeds to the reduction of some auxiliary rvs which can be removed without reducing the rate region. This simplifies the complexity of the optimization of the many variables present in the bound.

Outer bound The rate region stated in Theorem 4.1 implies the next outer bound:

$$R_1 \leq I(U_1;Y_1|TV_1) - I(U_1;Z|TV_1) \ , \quad (4.13)$$
$$R_2 \leq I(U_2;Y_2|TV_2) - I(U_2;Z|TV_2) \ , \quad (4.14)$$
$$R_1 + R_2 \leq I(X;Y_2|TZV_1) + I(U_1;Y_1|TV_1) - I(U_1;ZY_2|TV_1) \ , \quad (4.15)$$
$$R_1 + R_2 \leq I(X;Y_1|TZV_2) + I(U_2;Y_2|TV_2) - I(U_2;ZY_1|TV_2) \ , \quad (4.16)$$

for some joint input p.m.f $P_{TV_1V_2U_1U_2X}$.

Proof: The proof is relegated to Section 4.4.3. ■

It is easy to check that by removing the secrecy constraint, i.e., if Z is dropped, the above rate region reduces to the best known outer bound to the capacity of the standard BC [28, Lemma 3.5]. Moreover, this outer bound will prove to be crucial to characterize the secrecy capacity of several classes of WBCs, as will be stated later on.

4.1.2 Inner bound on the secrecy capacity region of the Wiretap BC

In this section, we present an inner bound on the secrecy capacity region of the WBC. The coding argument combines both stochastic encoding to achieve secrecy and the standard coding techniques for the BC, i.e., superposition coding and random binning to let the sent codewords be arbitrarily dependent.

Theorem 36 (Inner bound)**.** *The secrecy capacity region of the WBC includes all rate pairs* (R_1, R_2) *satisfying:*

$$R_1 \leq I(QU_1;Y_1|T) - I(QU_1;Z|T) \ , \quad (4.17)$$
$$R_2 \leq I(QU_2;Y_2|T) - I(QU_2;Z|T) \ , \quad (4.18)$$
$$R_1 + R_2 \leq I(U_1;Y_1|TQ) + I(QU_2;Y_2|T) - I(QU_1U_2;Z|T) - I(U_1;U_2|TQ) \ , \quad (4.19)$$
$$R_1 + R_2 \leq I(U_2;Y_2|TQ) + I(QU_1;Y_1|T) - I(QU_1U_2;Z|T) - I(U_1;U_2|TQ) \ , \quad (4.20)$$
$$R_1 + R_2 \leq I(QU_1;Y_1|T) + I(QU_2;Y_2|T) - I(QU_1U_2;Z|T) - I(U_1;U_2|TQ) - I(Q;Z|T) \ , \quad (4.21)$$

for some joint p.m.f $P_{TQU_1U_2X}$ *such that* $(T, Q, U_1, U_2) \multimap X \multimap (Y_1, Y_2, Z)$.

Proof: The full proof of this inner bound is given in Section 4.5. ■

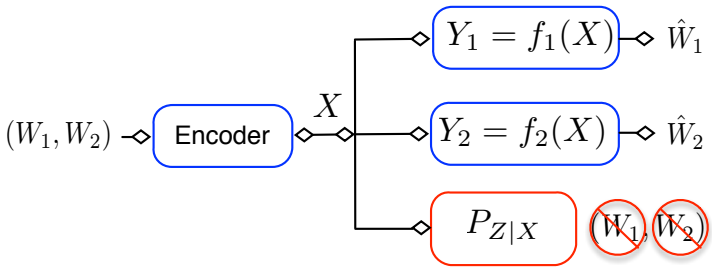


Figure 4.1: Deterministic BC with an arbitrary eavesdropper.

4.2 Secrecy Capacity of Some Wiretap BCs

In this section, we derive the secrecy capacity of various Wiretap Broadcast Channel models.

4.2.1 Deterministic BC with an arbitrary eavesdropper

Let us assume that both legitimate users' channel outputs are deterministic functions of the input X, as shown in Fig. 4.1.

Theorem 37 (Secrecy capacity of the deterministic BC with a general eavesdropper)**.** *The secrecy capacity of the deterministic BC with an arbitrary eavesdropper's channel is given by the set of all rate pairs (R_1, R_2) satisfying:*

$$R_1 \leq H(Y_1|Z) \ , \tag{4.22}$$
$$R_2 \leq H(Y_2|Z) \ , \tag{4.23}$$
$$R_1 + R_2 \leq H(Y_1Y_2|Z) \ , \tag{4.24}$$

for some input p.m.f P_X.

Proof. We start with the achievability part for which we evaluate the inner bound in Theorem 36 by setting: $Q = \emptyset$, $U_1 = Y_1$ and $U_2 = Y_2$. The claim follows then in a straightforward manner. As for the outer bound, it follows from the reduced outer bound in Corollary 35, by writing the next set of inequalities for $j \in \{1, 2\}$:

$$\begin{aligned} I(U_j; Y_j|V_j) - I(U_j; Z|V_j) &\leq I(U_j; Y_jZ|V_j) - I(U_j; Z|V_j) && (4.25)\\ &= I(U_j; Y_j|Z, V_j) && (4.26)\\ &\leq H(Y_j|Z) && (4.27) \end{aligned}$$

with strict equality if $U_j = Y_j$ and $V_j = \emptyset$. Note also that:

$$\begin{aligned} I(X; Y_2|ZV_1) + I(U_1; Y_1|V_1) - I(U_1; ZY_2|V_1) &\leq I(X; Y_2|ZV_1) + I(U_1; Y_1|ZY_2V_1) && (4.28)\\ &\leq H(Y_2|ZV_1) + H(Y_1|ZY_2V_1) && (4.29)\\ &\leq H(Y_1Y_2|Z) && (4.30) \end{aligned}$$

with strict equality if $U_1 = Y_1$ and $V_1 = \emptyset$. The second sum-rate yields the same constraint. Thus, the outer bound is maximized with the choice $U_1 = Y_1$, $U_2 = Y_2$ and $V_1 = V_2 = \emptyset$. □

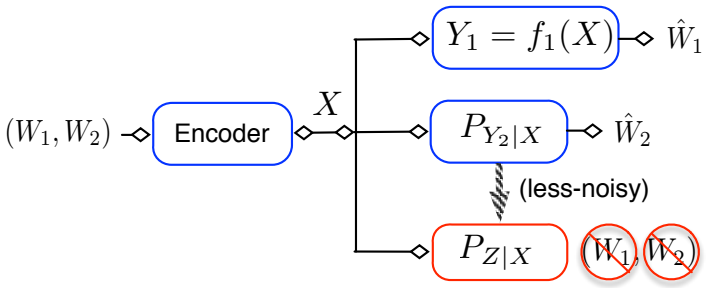


Figure 4.2: The Semi-deterministic Wiretap Broadcast Channel with a more-noisy eavesdropper.

Below, we generalize the equality between the regions in Corollary 35 and Theorem 36 to the case of the Semi-Deterministic BC with a more-noisy eavesdropper.

4.2.2 Semi-deterministic BC with a more-noisy eavesdropper

Let us assume that only Y_1 is a deterministic function of X but we further assume that Y_2 is less-noisy respect to the eavesdropper's output Z, as shown in Fig. 4.2.

Theorem 38 (Secrecy capacity region of the semi-deterministic BC with a more-noisy eavesdropper)**.** *The secrecy capacity of the semi-deterministic BC with a more-noisy eavesdropper is the set of all rate pairs (R_1, R_2) satisfying:*

$$R_1 \leq H(Y_1|ZQ) \ , \tag{4.31}$$
$$R_2 \leq I(U;Y_2|Q) - I(U;Z|Q) \ , \tag{4.32}$$
$$R_1 + R_2 \leq H(Y_1|ZQU) + I(U;Y_2|Q) - I(U;Z|Q) \tag{4.33}$$

for some joint p.m.f $P_{QUX} = P_Q P_{U|Q} P_{X|U}$ such that $(Q,U) \multimap X \multimap (Y_1, Y_2, Z)$.

Proof. Achievability follows from the rate region stated in Theorem 36 by letting: $Q = T$ and $U_1 = Y_1$. As for the converse, we will first evaluate the outer bound given in Corollary 35. Since Y_2 is less-noisy than Z, then one can easily notice that:

$$I(U;Y_2|VQ) - I(U;Z|VQ) \leq I(UV;Y_2|Q) - I(UV;Z|Q) \ . \tag{4.34}$$

Considering the same chain of inequalities as in (4.26)-(4.27), one can write the outer bound as:

$$R_1 \leq H(Y_1|ZQ) \ , \tag{4.35}$$
$$R_2 \leq I(UV;Y_2|Q) - I(UV;Z|Q) \ , \tag{4.36}$$
$$R_1 + R_2 \leq H(Y_1|ZQUV) + I(UV;Y_2|Q) - I(UV;Z|Q) \ , \tag{4.37}$$

and thus, defining $(UV) = U$, we can write that the outer bound is the union over all p.m.f $P_{QUX} = P_Q P_{U|Q} P_{X|U}$ of the rate region given in Theorem 38. □

Remarks 39. *When Y_2 is not less-noisy than Z, it is not clear yet whether the two bounds can be tight due to the fact that the auxiliary rv V does not seem to be useless then.*

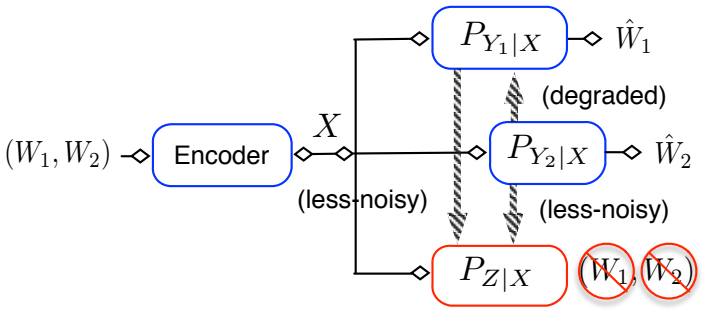


Figure 4.3: Degraded BC with a more-noisy eavesdropper.

4.2.3 Degraded BC with a more-noisy eavesdropper

In this section, we assume that the legitimate user Y_2 is degraded respect to the legitimate user Y_1. Moreover, assume that both users are less-noisy than the eavesdropper as shown in Fig. 4.3. The capacity region of this setting was first derived in [24], and here, we simply rely on the optimality of our outer bound for this setting.

Theorem 40 (Secrecy capacity region of the degraded WBC [24])**.** *The secrecy capacity region of the degraded WBC is given by the set of rate pairs* (R_1, R_2) *satisfying:*

$$R_1 \leq I(X;Y_1|TU) - I(X;Z|TU) \ , \tag{4.38}$$
$$R_2 \leq I(U;Y_2|T) - I(U;Z|T) \ , \tag{4.39}$$

for some input p.m.f P_{TUX} *where* $(T,U) \multimap X \multimap (Y_1, Y_2, Z)$.

Proof. To show this, we first note that the outer bound given in Theorem 35 is included in the following outer bound obtained through keeping only the constraints:

$$R_1 \leq I(U_1;Y_1Y_2|TV_1U_2V_2) - I(U_1;Z|TV_1U_2V_2) \ , \tag{4.40}$$
$$R_2 \leq I(U_2;Y_2|TV_2) - I(U_2;Z|TV_2) \ . \tag{4.41}$$

Now, since Y_2 is degraded respect to Y_1, then

$$I(U_1;Y_1Y_2|TV_1U_2V_2) = I(U_1;Y_1|TV_1U_2V_2) \ , \tag{4.42}$$

and since Y_1 is less-noisy than Z we can write

$$I(U_1;Y_1|TV_1U_2V_2) - I(U_1;Z|TV_1U_2V_2) \leq I(U_1V_1;Y_1|TV_1U_2) - I(U_1V_1;Z|TU_2V_2) \tag{4.43}$$
$$\leq I(X;Y_1|TU_2V_2) - I(X;Z|TU_2V_2) \ . \tag{4.44}$$

Thus, the outer bound reduces to the union over all joint p.m.fs P_{TUX} of the rate region given in Theorem 40. □

In the sequel, it turns out that the outer bound we derived yields also the capacity region of another class of ordered BC, which does not include the class of degraded BC with a more-noisy eavesdropper as will be clarified shortly.

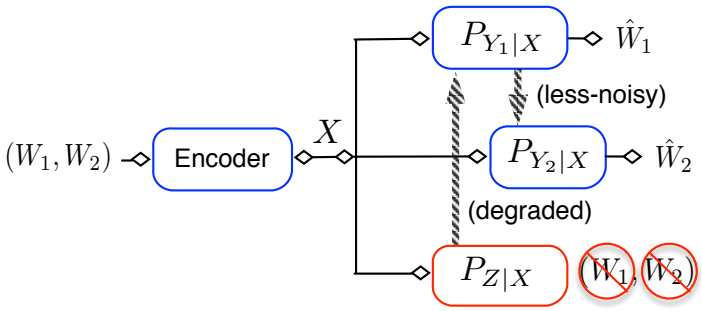


Figure 4.4: Less-Noisy BC with a partly degraded eavesdropper.

4.2.4 Less-Noisy BC with a partly degraded eavesdropper

Let us assume that Y_1 is a less-noisy channel than Y_2 and that Z is a degraded version of Y_1. As shown in Fig. 4.4, this model is more general than the one first considered in [23], while it does not really generalize the model in Fig. 4.3, first considered in [24]. Notice that in this setting the eavesdropper is not compulsorily degraded. However, the present class is wider in that users are no longer compulsorily degraded between them and the eavesdropper is no longer more noisy than the weaker legitimate user.

Theorem 41 (Secrecy capacity region of the less-noisy WBC)**.** *The secrecy capacity region of the ordered WBC under study is the set of all rate pairs* (R_1, R_2) *satisfying:*

$$R_2 \leq I(U;Y_2|T) - I(U;Z|T) \ , \tag{4.45}$$

$$R_1 + R_2 \leq I(X;Y_1|ZUT) + I(U;Y_2|T) - I(U;Z|T) \ , \tag{4.46}$$

for some joint p.m.f $P_{TUX} = P_T P_{U|T} P_{X|U}$ *such that* $(T,U) \multimap X \multimap (Y_1, Y_2, Z)$.

Proof. The converse follows from the outer bound in Corollary 35 by keeping only the terms:

$$R_2 \leq I(U_2;Y_2|TV_2) - I(U_2;Z|TV_2) \ , \tag{4.47}$$

$$R_1 + R_2 \leq I(X;Y_1|TZU_2V_2) + I(U_2;Y_2|TV_2) - I(U_2;ZY_1|TV_2) \ , \tag{4.48}$$

and defining the common auxiliary rv $T \equiv (T, V_2)$. As for the achievability, let $U_1 = X$ and $Q = U_2$ in the inner bound given by Theorem 36. This bound reduces to:

$$R_1 \leq I(X;Y_1|T) - I(X;Z|T) = I(X;Y_1|ZT) \ , \tag{4.49}$$

$$R_2 \leq I(U;Y_2|T) - I(U;Z|T) \ , \tag{4.50}$$

$$R_1 + R_2 \leq I(X;Y_1|ZUT) + I(U;Y_2|T) - I(U;Z|T) \ , \tag{4.51}$$

$$R_1 + R_2 \leq I(X;Y_1|T) - I(X;Z|T) = I(X;Y_1|ZT) \ . \tag{4.52}$$

The first bound is redundant with respect to the last one. Moreover, since Y_1 is less-noisy than Y_2, then the bound (4.52) becomes redundant with respect to (4.51). The inner bound reduces henceforth to the one given in Theorem 41. □

In the sequel, we study a non-straightforward extension of this WBC for which the secrecy capacity region remained open since the previous results in literature apply only to the degraded BC case.

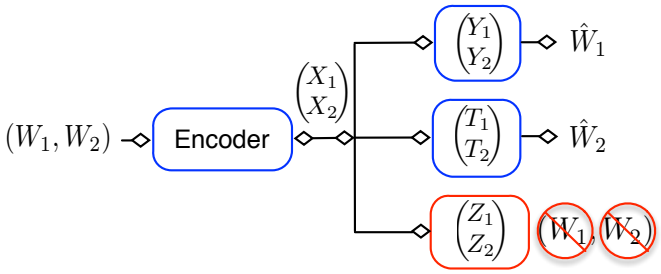


Figure 4.5: The Parallel Broadcast Channel (PBC) with an eavesdropper.

4.2.5 Product of two Inversely Less-Noisy Wiretap BCs

The product of inversely less-noisy broadcast channels is defined as the product of two less-noisy WBCs. The BC (Y_1, T_1) has a component Y_1 which is less-noisy than T_1 and an eavesdropper Z_1 is degraded towards the best user Y_1 and more-noisy than the worst user T_1. The BC (Y_2, T_2) is less-noisy in the inverse order and the eavesdropper Z_2 is degraded towards T_2 and more-noisy than Y_2.

Theorem 42 (Product of two inversely less-noisy BCs with a more-noisy eavesdropper)**.** *The secrecy capacity region of such a setting is given by the set of rates pairs* (R_1, R_2) *satisfying:*

$$R_1 \leq I(X_1; Y_1|Z_1) + I(U_2; Y_2) - I(U_2; Z_2) \ , \tag{4.53}$$
$$R_2 \leq I(X_2; T_2|Z_2) + I(U_1; T_1) - I(U_1; Z_1) \ , \tag{4.54}$$
$$R_1 + R_2 \leq I(X_1; Y_1|Z_1) + I(U_2; Y_2) - I(U_2; Z_2) + I(X_2; T_2|Z_2U_2) \ , \tag{4.55}$$
$$R_1 + R_2 \leq I(X_2; T_2|Z_2) + I(U_1; T_1) - I(U_1; Z_1) + I(X_1; Y_1|Z_1U_1) \ , \tag{4.56}$$

for some input p.m.f $P_{U_1X_1U_2X_2} = P_{U_1X_1}P_{U_2X_2}$ *that satisfies* $(U_1, U_2) \multimap (X_1, X_2) \multimap (Y_1, Y_2, T_1, T_2, Z_1, Z_2)$.

Proof. The proof is quite evolved in that it requires a new outer bound formulation, and is thus relegated to Appendix E.6. □

Note here that, in the absence of the eavesdropper, this theorem yields the capacity region of the product of two reversely less-noisy BCs which, though not proved in [12], can be deducted from the result of [62] for the product of reversely more-capable BCs.

4.3 The BEC/BSC Broadcast Channel with a BSC eavesdropper

In this section, we characterize the capacity region of the BEC/BSC broadcast channel with an external BSC eavesdropper. This model falls into the class of ordered BCs and is extremely rich since the BC (BEC and BSC) provides for a variety of orderings following the respective values of the erasure probability "e" and the crossover probability "p", as

$0 \leq e \leq 2p$	$2p < e \leq 4p(1-p)$	$4p(1-p) < e \leq h(p)$	$h(p) < e \leq 1$
BSC degraded of BEC	BEC Less Noisy BSC	BEC More Capable BSC	BSC Ess. Less Noisy BEC

Table 4.1: Different Orderings allowed by the BEC(e)/BSC(p) BC.

it is summarized in the table 4.1 and shown in [29]. Let us consider the channel model where:

$$\mathcal{W} : \left\{ \begin{array}{lcl} \mathcal{X} & \longmapsto & \mathcal{Y}_1 \equiv \mathrm{BEC}(e)\,, \\ \mathcal{X} & \longmapsto & \mathcal{Y}_2 \equiv \mathrm{BSC}(p_2)\,, \\ \mathcal{X} & \longmapsto & \mathcal{Z} \equiv \mathrm{BSC(p)}\,. \end{array} \right. \tag{4.57}$$

We will consider the case where Y_1 is less-noisy that Y_2 and where Z is degraded towards Y_2. Besides, we make sure that Z is degraded towards Y_1. [4] Summarizing these constraints, we end up with the inequalities:

$$2p_2 \leq e \leq \min\{2p, 4p_2(1-p_2)\}\ . \tag{4.58}$$

Theorem 43 (Secrecy capacity region of the BEC(e) /BSC(p_2) BC with BSC(p) eavesdropper)**.** *The capacity region of the BC with BEC(e) / BSC(p_2) components and a BSC(p) eavesdropper, defined by the constraint* (4.58) *where* $1-4p(1-p) \geq 4p_2(1-p_2)$*, is given by the set of rate pairs satisfying:*

$$\mathcal{C} : \left\{ \begin{array}{lcl} R_1 & \leq & (1-e)\, h_2(x) + h_2(p) - h_2(p \star x)\ , \\ R_2 & \leq & h_2(p \star x) - h_2(p_2 \star x)\ , \end{array} \right. \tag{4.59}$$

for some $x \in [0 : 0.5]$.

Proof. The proof consists in evaluating the capacity region of such an ordered channel given by the set of rate pairs (R_1, R_2) satisfying:

$$\mathcal{R} : \left\{ \begin{array}{lcl} R_1 & \leq & I(X;Y_1|TU) - I(X;Z|TU) = I(X;Y_1|ZTU)\ , \\ R_2 & \leq & I(U;Y_2|T) - I(U;Z|T) = I(U;Y_2|ZT)\ , \end{array} \right. \tag{4.60}$$

and is two fold. The challenging part is obviously the converse part since it requires the use of an inequality, similar in a way to Mrs. Gerber's lemma [61] applied to the secrecy capacity region, which we have been able to prove only under the assumption $1-4p(1-p) \geq 4p_2(1-p_2)$, although there is strong evidence that the converse can be proved besides this case.

Note that $T = \emptyset$ maximizes the region since it can easily be shown to be convex and thus, will not need the time-sharing variable T. Moreover, we can state a cardinality bound on the auxiliary rv U used in evaluating the previous region following the usual Fenchel-Eggleston-Caratheodory theorem that is it suffices to evaluate the region using an auxiliary rv with a quaternary alphabet.

[4] It is worth emphasizing here that our choice of Z degraded respect to Y_2 follows from that both channels are naturally degraded since these are *BSC* channels. Otherwise, if Y_2 were to be degraded respect to Z, no positive rate could be transmitted to user 2.

First, note that the choice $X = U \oplus V$ where $U \sim \text{Bern}(0.5)$, $V \sim \text{Bern}(x)$ yields that $X \sim \text{Bern}(0.5)$ and that $X|U \sim \text{Bern}(x)$. Thus, we can write:

$$I(X;Y_1|U) = (1-e)H(X|U) = (1-e)h_2(x) \ , \tag{4.61}$$
$$I(X;Z|U) = h_2(p*x) - h_2(p) \ , \tag{4.62}$$
$$I(U;Y_2) = 1 - h_2(p_2 * x) \ , \tag{4.63}$$
$$I(U;Z) = 1 - h_2(p*x) \ , \tag{4.64}$$

which proves the inclusion of the region $\mathcal{R}$ in the rate region $\mathcal{C}$, i.e., the achievability.

As for the inclusion in the appositive way, i.e., the converse, we will use the following lemma.

Lemma 2. *If $1 - 4p(1-p) \leq 4p_2(1-p_2)$, then $\mathcal{R}$ defines a convex set.*

Proof: The proof is given in Appendix E.4. ∎

Now, since $\mathcal{R}$ and $\mathcal{C}$ define convex bounded sets, then both are uniquely defined by their supporting hyperplanes. And finally, since $\mathcal{R}$ is included in $\mathcal{C}$, it thus suffices to show that all their supporting hyperplanes intersect, so let then $\lambda \in [0:\infty[$. We want to show that[5]:

$$\max_{(R_1,R_2)\in\mathcal{C}} R_1 + \lambda R_2 \leq \max_{(R_1,R_2)\in\mathcal{R}} R_1 + \lambda R_2 \ . \tag{4.65}$$

Let us choose the following notation: U is an auxiliary rv that takes its values in $\mathcal{U} = \{1, \dots, \|\mathcal{U}\|\}$ following the law: $\mathbb{P}(U=u) = P_U(u) \triangleq P_u$. Let us assume that X is a $\text{Bern}(\alpha)$ distributed Binary rv and that[6] $\mathbb{P}(X=0|U=u) = P_{X|U}(0|u) \triangleq x_u$.

Define the set $\mathcal{P}$ of admissible transition probabilities as:

$$\mathcal{P} \triangleq \Bigg\{ (\alpha, \mathbf{x}_{\|\mathcal{U}\|}, \mathbf{p}_{\|\mathcal{U}\|}) = (\alpha, x_1, \dots, x_{\|\mathcal{U}\|}, p_1, \dots, p_{\|\mathcal{U}\|}) \in [0:0.5]^{\|\mathcal{U}\|+1} \times [0:1]^{\|\mathcal{U}\|} \\ \sum_{u=1}^{\|\mathcal{U}\|} p_u = 1 \ , \ \sum_{u=1}^{\|\mathcal{U}\|} p_u x_u = \alpha \Bigg\} \ . \tag{4.66}$$

With this, note that:

$$\begin{aligned}
&\max_{(R_1,R_2)\in\mathcal{C}} R_1 + \lambda R_2 \\
&= \max_{\substack{P_{UX} \\ U \multimap X \multimap (Y_1,Y_2,Z)}} I(X;Y_1|U) - I(X;Z|U) + \lambda \Big[I(U;Y_2) - I(U;Z) \Big] && (4.67) \\
&= \max_{(\alpha\,,\,\mathbf{x}_{\|\mathcal{U}\|}\,,\,\mathbf{p}_{\|\mathcal{U}\|})\in\mathcal{P}} h_2(p) + \lambda \Big[h_2(p_2*\alpha) - h_2(p*\alpha) \Big] \\
&\quad + \sum_{u\in\mathcal{U}} P_u \Big\{ (1-e)h_2(x_u) - h_2(p*x_u) + \lambda \Big[h_2(p*x_u) - h_2(p_2*x_u) \Big] \Big\} && (4.68) \\
&\overset{(a)}{\leq} \max_{(\alpha\,,\,\mathbf{x}_{\|\mathcal{U}\|}\,,\,\mathbf{p}_{\|\mathcal{U}\|})\in\mathcal{P}} h_2(p)
\end{aligned}$$

[5] Note that the maxima are well defined for both regions due to the cardinality bound (for $\mathcal{C}$) and for the closed and bounded interval for $\mathcal{R}$ which results in compact supports for both optimizations.

[6] $\mathcal{U}$ is the support of the law P_U, as such, $P_{X|U}(0|u)$ is well defined.

$$+ \sum_{u\in\mathcal{U}} P_u \left\{(1-e)h_2(x_u) - h_2(p*x_u) + \lambda\Big[h_2(p*x_u) - h_2(p_2*x_u)\Big]\right\} \tag{4.69}$$

$$\overset{(b)}{\leq} h_2(p) + (1-e)h_2(x_u^\lambda) - h_2(p*x_u^\lambda) + \lambda\Big[h_2(p*x_u^\lambda) - h_2(p_2*x_u^\lambda)\Big] \tag{4.70}$$

$$= \max_{(R_1,R_2)\in\mathcal{R}} R_1 + \lambda R_2 \ , \tag{4.71}$$

where:

$$x_u^\lambda = \arg\max \left\{(1-e)h_2(x) - h_2(p*x) + \lambda\Big[h_2(p*x) - h_2(p_2*x)\Big]\right\} \ . \tag{4.72}$$

Now, (a) follows from the fact that since $x, p_1, p_2 \in [0:1/2]$ and $p \geq p_2$, then:

$$\forall \alpha \in [0:1/2] \qquad , \qquad p_2 * \alpha \leq p * \alpha \leq 1/2 \tag{4.73}$$

$$\text{then} \qquad \max_{\alpha\in[0:1/2]} [h_2(p_2*\alpha) - h_2(p*\alpha)] = 0 \tag{4.74}$$

with equality for $\alpha = 1/2$. As for (b), it is a direct result of the existence of a value of x_u^λ that maximizes the expression, and from that letting $\mathcal{U} = \{0,1\}$ and $P_0 = P_1 = \frac{1}{2}$ and $U \longmapsto X \equiv BSC(x_u^\lambda)$, leads to this maximum value equality in (b) in addition to being admissible: $P_0 x_u^\lambda + P_1(1-x_u^\lambda) = \alpha = \frac{1}{2}$. This ends the proof of equality of the two rate regions. □

In the sequel, we evaluate the effect of eavesdropping on such a BEC(e)/BSC(p_2) BC with a BSC(p) eavesdropper.

First note $\mathcal{C}_{std}$ the standard capacity region of the BC without an eavesdropper, $\mathcal{C}$ being its secrecy capacity region. We have that [29]:

$$\mathcal{C}_{std} : \begin{cases} R_1 & \leq & (1-e)\, h_2(x) \ , \\ R_2 & \leq & 1 - h_2(p_2 \star x) \ , \end{cases} \tag{4.75}$$

for some $x \in [0:0.5]$.

The presence of eavesdropper engenders an impediment on the sum rate given by $1 - h_2(p)$, that does not depend on the choice of the channel parameters (e, p_2). As such, it turns out that the channel to user 2 ,i.e. BSC(p_2) is very sensitive to such the BSC(p) eavesdropper in that it could have zero admissible rate R_2 if the eavesdropper were to have a channel as good as to allow for $p = p_2$. However, and that's peculiar to the BEC(e) channel, user 1 always has strictly positive rates whatever the value of p, since $e \leq 2p \leq h_2(p)$ and thus, a rate of $h_2(p) - 2p > 0$ is always achievable.

To illustrate this, we consider the following transmission scheme where $e = 2p$, i.e. the worst eavesdropper is considered for user 1, and where we vary p in the interval $[p_2 : 0.5]$. Fig. 4.6 plots the obtained curves. As expected, the eavesdropper has no impediment on the available rates for both users when p is close to 0.5, however, as p decreases, the gap between the standard capacity region and the secrecy capacity region increases, and the rate available at user 2 decreases to zero whilst that of user 1, stays above a given threshold.

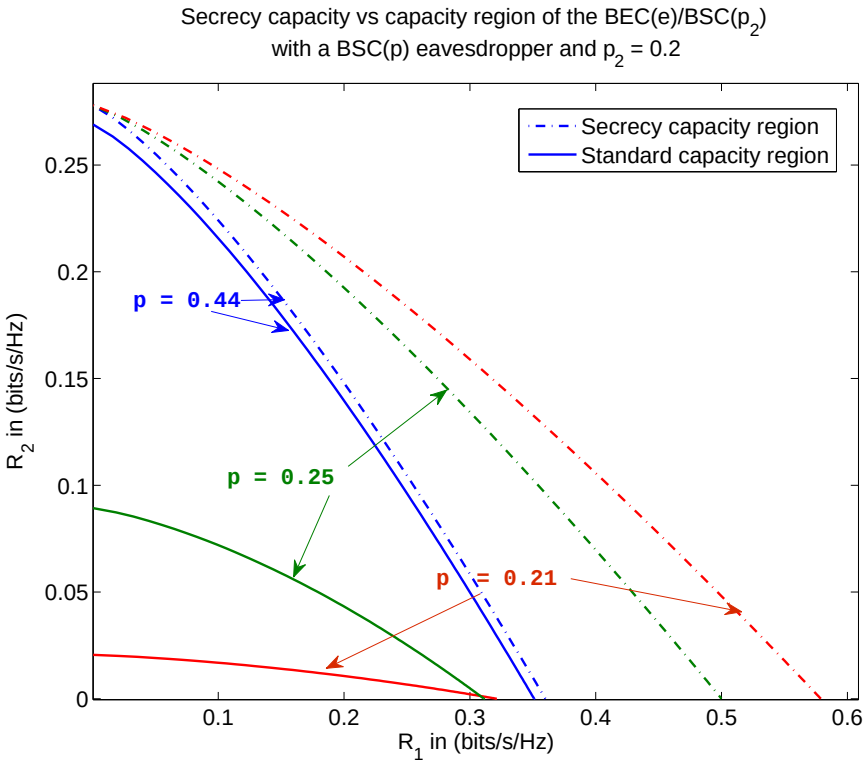


Figure 4.6: Secrecy capacity region of the BC with BEC(e)/BSC(p_2) components and a BSC(p) eavesdropper.

4.4 Proof of Theorem 35: Outer Bound

In this section, we prove the outer bound in Theorem 35, since this rate region is symmetric in the rates R_j, $j \in \{1, 2\}$, the constraints will be shown only for the following two single rates and two sum-rates:

$$R_1 \leq I(U_1; Y_1|TV_1) - I(U_1; Z|TV_1) \ , \tag{4.76}$$
$$R_1 \leq I(U_1; Y_1Y_2|TV_1V_2) - I(U_1; Z|TV_1V_2) \ , \tag{4.77}$$
$$R_1 + R_2 \leq I(X; Y_2|TZV_1) + I(U_1S_1; Y_1|TV_1) - I(U_1S_1; ZY_2|TV_1) \ , \tag{4.78}$$
$$R_1 + R_2 \leq I(X; Y_2|TZV_1V_2) + I(U_1S_1; Y_1Y_2|TV_1V_2) - I(U_1S_1; ZY_2|TV_1V_2) \ . \tag{4.79}$$

4.4.1 Single rates' constraints

By Fano's inequality we have that:

$$nR_1 \leq I(W_1; Y_1^n) + n\,\epsilon_n \ . \tag{4.80}$$

Moreover, from the secrecy constraint: $I(W_1; Z^n) \leq n\,\epsilon_n$. Thus, one can write that:

$$n\,R_1 \leq I(W_1; Y_1^n) - I(W_1; Z^n) + 2\,n\,\epsilon_n \tag{4.81}$$

$$= \sum_{i=1}^{n} \Big[I(W_1; Y_{1,i}|Y_1^{i-1}) - I(W_1; Z_i|Z_{i+1}^n) \Big] + 2\, n\, \epsilon_n \tag{4.82}$$

$$\overset{(a)}{=} \sum_{i=1}^{n} \Big[I(W_1 Z_{i+1}^n; Y_{1,i}|Y_1^{i-1}) - I(W_1 Y_1^{i-1}; Z_i|Z_{i+1}^n) \Big] + 2\, n\, \epsilon_n \tag{4.83}$$

$$\overset{(b)}{=} \sum_{i=1}^{n} \Big[I(W_1; Y_{1,i}|Y_1^{i-1} Z_{i+1}^n) - I(W_1; Z_i|Y_1^{i-1} Z_{i+1}^n) \Big] + 2\, n\, \epsilon_n \ , \tag{4.84}$$

where (a) and (b) follow both from the Csiszár & Körner's sum-identity (A.1):

$$\sum_{i=1}^{n} \Big[I(Z_{i+1}^n; Y_{1,i}|W_1 Y_1^{i-1}) - I(Y_1^{i-1}; Z_i|W_1 Z_{i+1}^n) \Big] = 0 \ , \tag{4.85}$$

$$\sum_{i=1}^{n} \Big[I(Z_{i+1}^n; Y_{1,i}|Y_1^{i-1}) - I(Y_1^{i-1}; Z_i|Z_{i+1}^n) \Big] = 0 \ . \tag{4.86}$$

We then define: $U_{1,i} = W_1$, $V_{1,i} = Y_1^{i-1}$ and $T_i = Z_{i+1}^n$, which yields the first single rate constraint.

In the same fashion, we can write the other single rates by treating the two outputs Y_1 and Y_2 together, i.e $Y_1 \sim (Y_1, Y_2)$ letting $V_{2,i} = Y_2^{i-1}$. We end up with the couple of constraints:

$$\begin{cases} R_1 \ \leq \ I(U_1; Y_1|TV_1) - I(U_1; Z|TV_1) \ , \\ R_1 \ \leq \ I(U_1; Y_1 Y_2|TV_1V_2) - I(U_1; Z|TV_1V_2) \ . \end{cases} \tag{4.87}$$

Furthermore, similar all manipulations can be performed by starting from the Fano's inequality and secrecy requirement:

$$nR_1 \leq I(W_1; Y_1^n|W_2) - I(W_1; Z^n|W_2) + n\, \epsilon_n \ . \tag{4.88}$$

Thus, we could condition over $U_{2,i} = W_2$ the two previous rate constraints to obtain:

$$\begin{cases} R_1 \ \leq \ I(U_1; Y_1|TV_1U_2) - I(U_1; Z|TV_1U_2) \ , \\ R_1 \ \leq \ I(U_1; Y_1Y_2|TV_1U_2V_2) - I(U_1; Z|TV_1U_2V_2) \ . \end{cases} \tag{4.89}$$

4.4.2 Sum-rate constraints

Let us start by Fano's inequality writing:

$$n\, R_1 \leq I(W_1; Y_1^n) - I(W_1; Y_2^n Z^n) + I(W_1; Y_2^n Z^n) + n\, \epsilon_n \ . \tag{4.90}$$

Then, combining with the following constraint obtained from Fano's inequality:

$$n\, R_2 \leq I(W_2; Y_2^n Z^n|W_1) + n\, \epsilon_n \ , \tag{4.91}$$

we can write:

$$n\, (R_1 + R_2) \leq I(W_1; Y_1^n) - I(W_1; Y_2^n Z^n) + I(W_1 W_2; Y_2^n Z^n) + 2n\, \epsilon_n \ . \tag{4.92}$$

Now, let us elaborate on that:

$$I(W_1; Y_1^n) - I(W_1; Y_2^n Z^n)$$

$$= \sum_{i=1}^{n} \Big[I(W_1; Y_{1,i}|Y_1^{i-1}) - I(W_1; Y_{2,i}Z_i|Y_{2,i+1}^n Z_{i+1}^n) \Big] \tag{4.93}$$

$$\overset{(a)}{=} \sum_{i=1}^{n} \Big[I(W_1 Y_{2,i+1}^n Z_{i+1}^n; Y_{1,i}|Y_1^{i-1}) - I(W_1 Y_1^{i-1}; Y_{2,i}Z_i|Y_{2,i+1}^n Z_{i+1}^n) \Big] \tag{4.94}$$

$$= \sum_{i=1}^{n} \Big[I(W_1 Y_1^{i-1} Y_{2,i+1}^n Z_{i+1}^n; Y_{1,i}) - I(W_1 Y_1^{i-1} Y_{2,i+1}^n Z_{i+1}^n; Y_{2,i}Z_i) + I(Y_{2,i+1}^n Z_{i+1}^n; Y_{2,i}Z_i) - I(Y_1^{i-1}; Y_{1,i}) \Big] \ , \tag{4.95}$$

where (a) is again a consequence of Csiszár & Körner's sum-identity (A.1):

$$\sum_{i=1}^{n} \Big[I(Z_{i+1}^n; Y_{1,i}|W_1 Y_1^{i-1}) - I(Y_1^{i-1}; Y_{2,i}Z_i|W_1 Y_{2,i+1}^n Z_{i+1}^n) \Big] = 0 \ . \tag{4.96}$$

As for the other term, note that:

$$I(W_1W_2; Y_2^n Z^n) = \sum_{i=1}^{n} \Big[I(W_1W_2 Y_{2,i+1}^n Z_{i+1}^n; Y_{2,i}Z_i) - I(Y_{2,i+1}^n Z_{i+1}^n; Y_{2,i}Z_i) \Big] \ . \tag{4.97}$$

Looking at the first term of the last equality:

$$\sum_{i=1}^{n} I(W_1W_2 Y_{2,i+1}^n Z_{i+1}^n; Y_{2,i}Z_i)$$

$$= \sum_{i=1}^{n} \Big[I(W_1W_2 Y_{2,i+1}^n Z_{i+1}^n Z^{i-1}; Y_{2,i}Z_i) - I(Z^{i-1}; Y_{2,i}Z_i|W_1W_2 Y_{2,i+1}^n Z_{i+1}^n) \Big] \tag{4.98}$$

$$= \sum_{i=1}^{n} \Big[I(W_1W_2 Y_{2,i+1}^n Z_{i+1}^n Z^{i-1}; Y_{2,i}Z_i) - I(Y_{2,i+1}^n Z_{i+1}^n; Z_i|W_1W_2 Z^{i-1}) \Big] \tag{4.99}$$

$$= \sum_{i=1}^{n} \Big[I(W_1W_2 Z^{i-1}; Z_i) + I(W_1W_2 Y_{2,i+1}^n Z_{i+1}^n Z^{i-1}; Y_{2,i}|Z_i) \Big] \tag{4.100}$$

$$= \sum_{i=1}^{n} \Big[I(W_1W_2; Z_i|Z^{i-1}) + I(Z^{i-1}; Z_i) + I(W_1W_2 Y_{2,i+1}^n Z_{i+1}^n Z^{i-1}; Y_{2,i}|Z_i) \Big] \ . \tag{4.101}$$

Here, (a) is a consequence of Csiszár & Körner's sum-identity (A.1) but between the outputs Z and (Y_2, Z):

$$\sum_{i=1}^{n} \Big[I(Z^{i-1}; Y_{2,i}Z_i|W_1W_2 Y_{2,i+1}^n Z_{i+1}^n) - I(Y_{2,i+1}^n Z_{i+1}^n; Z_i|W_1W_2 Z^{i-1}) \Big] = 0 \ . \tag{4.102}$$

Using the secrecy constraint, one can then notice that:

$$\sum_{i=1}^{n} I(W_1W_2; Z_i|Z^{i-1}) = I(W_1W_2; Z^n) \leq n\,\epsilon_n \ . \tag{4.103}$$

Moreover, observe that:

$$\sum_{i=1}^{n} I(Z^{i-1}; Z_i) = \sum_{i=1}^{n} I(Z_{i+1}^n; Z_i) \ , \tag{4.104}$$

and

$$I(W_1W_2Y_{2,i+1}^nZ_{i+1}^nZ^{i-1};Y_{2,i}|Z_i) \leq I(W_1W_2Y_{2,i+1}^nZ_{i+1}^nY_1^{i-1}Z^{i-1};Y_{2,i}|Z_i)\ . \tag{4.105}$$

The sum-rate can be then bounded as follows:

$$\begin{aligned} n\,(R_1+R_2) &\leq I(W_1;Y_1^n) - I(W_1;Y_2^nZ^n) + I(W_1W_2;Y_2^nZ^n) + 2n\,\epsilon_n & (4.106)\\ &\leq \sum_{i=1}^{n}\Big[I(W_1Y_1^{i-1}Y_{2,i+1}^nZ_{i+1}^n;Y_{1,i}) - I(W_1Y_1^{i-1}Y_{2,i+1}^nZ_{i+1}^n;Y_{2,i}Z_i)\\ &\quad + I(W_1W_2Y_{2,i+1}^nZ_{i+1}^nY_1^{i-1}Z^{i-1};Y_{2,i}|Z_i)\\ &\quad +\ I(Z_{i+1}^n;Z_i) - I(Y_1^{i-1};Y_{1,i})\Big] + 2n\,\epsilon_n. & (4.107)\end{aligned}$$

And to end, we use the following remarks:

$$\begin{aligned}\sum_{i=1}^{n}\Big[I(Z_{i+1}^n;Z_i) - I(Y_1^{i-1};Y_{1,i})\Big] &= \sum_{i=1}^{n}\Big[I(Y_1^{i-1}Z_{i+1}^n;Z_i) - I(Y_1^{i-1}Z_{i+1}^n;Y_{1,i})\Big] & (4.108)\\ &= \sum_{i=1}^{n}\Big[I(Y_1^{i-1}Z_{i+1}^n;Y_{2,i}Z_i) - I(Y_1^{i-1}Z_{i+1}^n;Y_{1,i})\\ &\qquad -I(Y_1^{i-1}Z_{i+1}^n;Y_{2,i}|Z_i)\Big]\ . & (4.109)\end{aligned}$$

Thus, combining with the previous equality, we end up with:

$$\begin{aligned} n\,(R_1+R_2) &\leq I(W_1;Y_1^n) - I(W_1;Y_2^nZ^n) + I(W_1W_2;Y_2^nZ^n) + 2n\,\epsilon_n & (4.110)\\ &\leq \sum_{i=1}^{n}\Big[I(W_1Y_1^{i-1}Y_{2,i+1}^nZ_{i+1}^n;Y_{1,i}) - I(Y_1^{i-1}Z_{i+1}^n;Y_{1,i})\\ &\qquad -I(W_1Y_1^{i-1}Y_{2,i+1}^nZ_{i+1}^n;Y_{2,i}Z_i) + I(Y_1^{i-1}Z_{i+1}^n;Y_{2,i}Z_i)\\ &\quad + I(W_1W_2Y_{2,i+1}^nY_1^{i-1}Z_{i+1}^nZ^{i-1};Y_{2,i}|Z_i) - I(Y_1^{i-1}Z_{i+1}^n;Y_{2,i}|Z_i)\Big] + 2n\,\epsilon_n & (4.111)\\ &\leq \sum_{i=1}^{n}\Big[I(W_1Y_{2,i+1}^n;Y_{1,i}|Y_1^{i-1}Z_{i+1}^n) - I(W_1Y_{2,i+1}^n;Y_{2,i}Z_i|Y_1^{i-1}Z_{i+1}^n)\\ &\qquad + I(X_i;Y_{2,i}|Z_iY_1^{i-1}Z_{i+1}^n)\Big] + 2n\,\epsilon_n\ . & (4.112)\end{aligned}$$

Letting: $S_{1,i} = Y_{2,i+1}^n$, $U_{1,i} = W_1$, $V_{1,i} = Y_1^{i-1}$, and $T_i = Z_{i+1}^n$, by resorting to a standard time-sharing argument we end up with the following single-letter constraint:

$$R_1 + R_2 \leq I(U_1S_1;Y_1|V_1T) - I(U_1S_1;Y_2Z|V_1T) + I(X_i;Y_2|ZV_1T)\ . \tag{4.113}$$

Similarly, we can show the same sum-rate constraint, by replacing the output Y_1 with the two outputs (Y_1Y_2), which results in:

$$R_1 + R_2 \leq I(X;Y_2|TZV_1V_2) + I(U_1S_1;Y_1Y_2|TV_1V_2) - I(U_1S_1;ZY_2|TV_1V_2)\ . \tag{4.114}$$

4.4.3 Proof of Corollary 35

In the previous section, we found that an outer bound on the secrecy region for the Wiretap BC can be obtained by considering only the constraints:

$$R_1 \leq I(U_1;Y_1|TV_1) - I(U_1;Z|TV_1)\ , \tag{4.115}$$

$$R_2 \leq I(U_2;Y_2|TV_2) - I(U_2;Z|TV_2) \ , \tag{4.116}$$
$$R_1 + R_2 \leq I(X;Y_2|TZV_1) + I(U_1S_1;Y_1|TV_1) - I(U_1S_1;ZY_2|TV_1) \ , \tag{4.117}$$
$$R_1 + R_2 \leq I(X;Y_1|TZV_2) + I(U_2S_2;Y_2|TV_2) - I(U_2S_2;ZY_1|TV_2) \ . \tag{4.118}$$

An important claim is then that the auxiliary rvs S_1 and S_2 can be eliminated with no impediment to the rate region. Since the region is symmetric in R_1 and R_2, we only show the claim for S_1. We are looking for a random variable $U_1^\star$ such that we can write:

$$R_1 \leq I(U_1^\star;Y_1|TV_1) - I(U_1^\star;Z|TV_1) \ , \tag{4.119}$$
$$R_1 + R_2 \leq I(X;Y_2|TZV_1) + I(U_1^\star;Y_1|TV_1) - I(U_1^\star;ZY_2|TV_1) \ . \tag{4.120}$$

To see this, define the two following functions:

$$f_1(Q) \triangleq I(U_1;Y_1|TV_1) - I(U_1;Z|TV_1) - I(Q;Y_1|TV_1) + I(Q;Z|TV_1) \ ,$$
$$f_2(Q) \triangleq I(U_1S_1;Y_1|TV_1) - I(U_1S_1;Y_2Z|TV_1) - I(Q;Y_1|TV_1) + I(Q;Y_2Z|TV_1) \ .$$

We note first that:

$$f_1(U_1) = 0 \quad , \quad f_2(U_1S_1) = 0 \ . \tag{4.121}$$

Moreover,

$$f_1(U_1S_1) + f_2(U_1) = -I(U_1S_1;Y_2|TZV_1) + I(U_1;Y_2|TZV_1) \tag{4.122}$$
$$= -I(S_1;Y_2|TZU_1V_1) \tag{4.123}$$
$$\leq 0 \ . \tag{4.124}$$

Therefore, either $f_1(U_1S_1) \leq 0$ and thus, letting $U_1^\star = (U_1S_1)$ will not reduce the region, or $f_1(U_1) \leq 0$ and in this case $U_1^\star = U$ allows us to prove our claim. The same holds for the other couple of constraints on R_2 and $R_1 + R_2$.

4.5 Proof of Theorem 36: Inner Bound

In this section, we prove the achievability of the inner bound stated in Theorem 36. Let R_1 and R_2 denote the information rates. Let T be any the time sharing random variable. The coding argument is as follows.

4.5.1 Code generation, encoding and decoding procedures

Rate splitting

We split the message intended to each user of rate R_j into two sub-messages: one of rate $\bar{R}_j = R_j - R_{0j}$ that will be decoded only by the user, and one of rate R_{0j} that will be carried through the common message. Thus in stead of transmitting the message pair (w_1, w_2), we transmit the triple $(\bar{w}_0, \bar{w}_1, \bar{w}_2)$.

$$\begin{cases} \bar{R}_0 & \triangleq & R_{01} + R_{02} \ , \\ \bar{R}_j & \triangleq & R_j - R_{0j} \geq 0 \ . \end{cases} \tag{4.125}$$

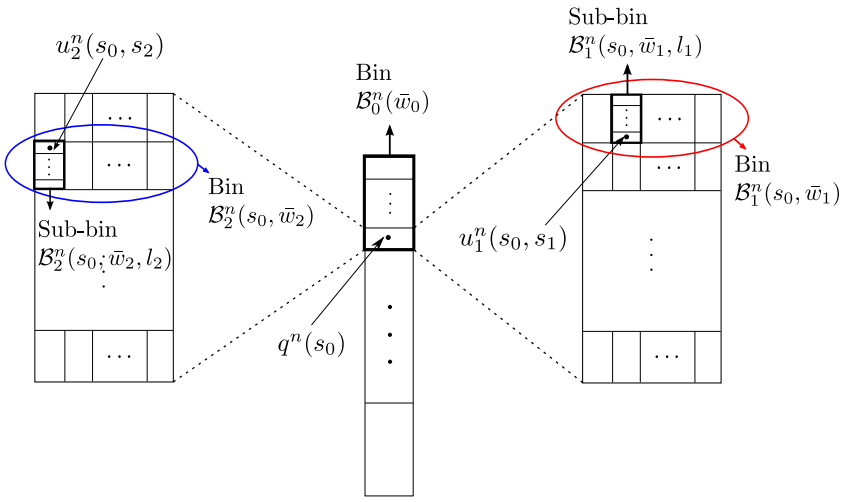


Figure 4.7: Codebook generation and encoding.

Codebook generation

Generate 2^{nT_0} sequences $q^n(s_0)$ following

$$P_Q^n(q^n(s_0)) = \prod_{i=1}^{n} P_Q(q_i^n(s_0)) \ , \tag{4.126}$$

where $T_0 \geq \bar{R}_0$ and map these in $2^{n\bar{R}_0}$ bins indexed by $\bar{w}_0$: $\mathcal{B}_0^n(\bar{w}_0)$.

For each $s_0 \in [1 : 2^{nT_0}]$ and for each $j \in \{1, 2\}$, generate 2^{nT_j} sequences $u_j^n(s_0, s_j)$ following

$$P_{U_j|Q}^n(u_j^n(s_0, s_j)|q^n(s_0)) = \prod_{i=1}^{n} P_{U_j|Q}(u_{j,i}^n(s_0, s_j)|q_i^n(s_0)) \ . \tag{4.127}$$

Map these sequences in $2^{n\bar{R}_j}$ bins indexed by $\bar{w}_j$: $\mathcal{B}_j^n(s_0, \bar{w}_j)$ and consisting in $2^{n(T_j - \bar{R}_j)}$ n-sequences. Each of these bins are divided into $2^{n\tilde{R}_j}$ sub-bins indexed by l_j: $\mathcal{B}_j^n(s_0, \bar{w}_j, l_j)$, thus each bin contains $2^{n(T_j - \bar{R}_j - \tilde{R}_j)}$ sequences where $0 \leq \tilde{R}_j \leq T_j - \bar{R}_j$.

The codebook consisting of all the bins is known to all terminals, including the eavesdropper.

Encoding

Fig. 4.7 plots the encoding operation. To send $(\bar{W}_0, \bar{W}_1, \bar{W}_2)$, the encoder selects at random an index s_0 such that $q^n(s_0) \in \mathcal{B}_0^n(\bar{w}_0)$. Then, in the product bin $\mathcal{B}_1^n(s_0, \bar{w}_1) \times \mathcal{B}_2^n(s_0, \bar{w}_2)$, it chooses at random a pair of sub-bins $\mathcal{B}_j^n(s_0, \bar{w}_1, l_1)$ and $\mathcal{B}_2^n(s_0, \bar{w}_2, l_2)$ indexed by l_1 and l_2. In the corresponding product sub-bin, it looks for a pair of sequences indexed with s_1 and s_2 satisfying:

$$(q^n(s_0), u_1^n(s_0, s_1), u_2^n(s_0, s_2)) \in T_\delta^n(QU_1U_2) \ . \tag{4.128}$$

Based on the Mutual Covering Lemma [63], the encoding will succeed if the following inequalities hold:

$$\begin{cases} T_1 - (\bar{R}_1 + \tilde{R}_1) + T_2 - (\bar{R}_2 + \tilde{R}_2) & > & I(U_1; U_2|Q) \ , \\ 0 & \leq & \tilde{R}_1 \leq T_1 - \bar{R}_1 \ , \\ 0 & \leq & \tilde{R}_2 \leq T_2 - \bar{R}_2 \ . \end{cases} \tag{4.129}$$

Decoding

Upon receiving y_j^n, decoder j looks jointly for a pair of indices (s_0, s_j) such that:

$$\left(q^n(s_0), u_j^n(s_0, s_j), y_j^n\right) \in T_\delta^n(QU_jY_j) \ . \tag{4.130}$$

From the decoded indices s_0 and s_j, it can infer the initial values of both $\bar{W}_0$ and $\bar{W}_j$.

Based on Lemma 8, the error probability can be made arbitrarily small provided that:

$$\begin{cases} T_j & \leq & I(U_j; Y_j|Q) \ , \\ T_j + T_0 & \leq & I(QU_j; Y_j) \ . \end{cases} \tag{4.131}$$

Equivocation analysis

We find conditions on the rates T_0, T_1, T_2 and $\tilde{R}_1, \tilde{R}_2$ to achieve perfect secrecy for all message triples $(\bar{W}_0, \bar{W}_1, \bar{W}_2)$.

To this end, we first note that it suffices to find conditions for which $\frac{1}{n} I(\bar{W}_0\bar{W}_1\bar{W}_2; Z^n|\mathcal{C})$ can be made arbitrarily small where $\mathcal{C}$ denotes the codebook used in the transmission, the latter constraint leading to the individual secrecy requirements being fulfilled.

Note that:

$$\begin{aligned} I(\bar{W}_0\bar{W}_1\bar{W}_2; Z^n|\mathcal{C}) &= n(\bar{R}_0 + \bar{R}_1 + \bar{R}_2) - H(\bar{W}_0\bar{W}_1\bar{W}_2|Z^n, \mathcal{C}) && (4.132) \\ &\overset{(a)}{=} n(\bar{R}_0 + \bar{R}_1 + \bar{R}_2) - H(S_0S_1S_2|Z^n, \mathcal{C}) \\ &\quad + H(S_0S_1S_2|Z^n\bar{W}_0\bar{W}_1\bar{W}_2, \mathcal{C}) \ , && (4.133) \end{aligned}$$

where (a) follows from that, knowing the codebook, the sent messages are deterministic functions of the binning indices chosen.

We first start by giving a lower bound to $H(S_0S_1S_2|Z^n, \mathcal{C})$. Let us write:

$$\begin{aligned} & H(S_0S_1S_2|Z^n, \mathcal{C}) \\ &= H(S_0|Z^n, \mathcal{C}) + H(S_1S_2|Z^n, S_0, \mathcal{C}) && (4.134) \\ &= H(S_0|\mathcal{C}) - I(S_0; Z^n|\mathcal{C}) + H(S_1S_2|S_0, \mathcal{C}) - I(S_1S_2; Z^n|S_0, \mathcal{C}) && (4.135) \\ &= nT_0 - I(S_0; Z^n|\mathcal{C}) + H(S_1S_2|S_0, \mathcal{C}) - I(S_1S_2; Z^n|S_0, \mathcal{C}) && (4.136) \\ &= n(T_0 + T_1 + T_2) - I(S_0; Z^n|\mathcal{C}) - I(S_1; S_2|S_0, \mathcal{C}) - I(S_1S_2; Z^n|S_0, \mathcal{C}) && (4.137) \\ &\overset{(a)}{=} n(T_0 + T_1 + T_2) - I(Q^n; Z^n|\mathcal{C}) - I(U_1^n; U_2^n|Q^n, \mathcal{C}) - I(U_1^nU_2^n; Z^n|Q^n, \mathcal{C}) \ , && (4.138) \end{aligned}$$

where (a) follows similarly from the fact that, knowing the codebook, the sent sequences are functions of the chosen binning indices.

The next lemma provides the main result for carrying on with the analysis.

Lemma 3. *Assuming the codebook generation presented before, the next inequalities hold true:*

$$I(Q^n; Z^n|\mathcal{C}) \leq nI(Q;Z) + n\,\epsilon_n \ , \tag{4.139}$$
$$I(U_1^n; U_2^n|Q^n, \mathcal{C}) \leq nI(U_1;U_2|Q) + n\,\epsilon_n \ , \tag{4.140}$$
$$I(U_1^n U_2^n; Z^n|Q^n, \mathcal{C}) \leq nI(U_1U_2;Z|Q) + n\,\epsilon_n \ . \tag{4.141}$$

Proof: The proof of this lemma is presented in Appendix E.1. ■

Lemma 3 allows us thus to write:

$$\frac{1}{n}H(S_0S_1S_2|Z^n, \mathcal{C}) \geq T_0 + T_1 + T_2 - I(U_1;U_2|Q) - I(QU_1U_2;Z) \ . \tag{4.142}$$

Now, let us upper bound the remainder term to be studied: $H(S_0S_1S_2|Z^n\bar{W}_0\bar{W}_1\bar{W}_2, \mathcal{C})$.

The following Lemma is useful to carry on with the proof.

Lemma 4. *Assuming the same coding scheme presented before, then*

$$\limsup_{n\to\infty} \frac{1}{n}H(S_0S_1S_2|Z^n\bar{W}_0\bar{W}_1\bar{W}_2, \mathcal{C}) \leq \max\{0, I_1, I_2, I_3, I_4\} \ , \tag{4.143}$$

where

$$I_1 = T_1 - \bar{R}_1 - I(U_1; ZU_2|Q) \ , \tag{4.144}$$
$$I_2 = T_2 - \bar{R}_2 - I(U_2; ZU_1|Q) \ , \tag{4.145}$$
$$I_3 = T_1 - \bar{R}_1 + T_2 - \bar{R}_2 - I(U_1U_2;Z|Q) - I(U_1;U_2|Q) \ , \tag{4.146}$$
$$I_4 = T_0 - \bar{R}_0 + T_1 - \bar{R}_1 + T_2 - \bar{R}_2 - I(QU_1U_2;Z) - I(U_1;U_2|Q) \ . \tag{4.147}$$

Proof: This Lemma is proved in Appendix E.2. ■

As a conclusion of this lemma, and combining (4.133) and (4.142) we can conclude that:

$$\begin{aligned}
&\frac{1}{n}I(\bar{W}_0\bar{W}_1\bar{W}_2; Z^n|\mathcal{C}) - \epsilon_n \\
&\leq \bar{R}_0 + \bar{R}_1 + \bar{R}_2 - (T_0 + T_1 + T_2) \\
&+ I(QU_1U_2;Z) + I(U_1;U_2|Q) + \max\{0, I_1, I_2, I_3, I_4\} \qquad (4.148)\\
&= \max\Big\{\bar{R}_0 + \bar{R}_1 + \bar{R}_2 - (T_0 + T_1 + T_2) + I(QU_1U_2;Z) + I(U_1;U_2|Q) \ , \\
&\qquad \bar{R}_0 - T_0 + \bar{R}_2 - T_2 + I(QU_2;Z) \ , \\
&\qquad \bar{R}_0 - T_0 + \bar{R}_1 - T_1 + I(QU_1;Z) \ , \\
&\qquad \bar{R}_0 - T_0 + I(Q;Z) \ , \ 0\Big\} \ . \qquad (4.149)
\end{aligned}$$

Hence, full secrecy is guaranteed by forcing all operands in the max term to be less than zero.

By collecting all inequalities and applying FME on the rates R_{01} and R_{02} (see details in Appendix E.3), we obtain the desired rate region:

$$R_1 \leq I(QU_1;Y_1) - I(QU_1;Z) \ , \tag{4.150}$$

$$R_2 \leq I(QU_2;Y_2) - I(QU_2;Z) \ , \tag{4.151}$$
$$R_1 + R_2 \leq I(U_1;Y_1|Q) + I(QU_2;Y_2) - I(QU_1U_2;Z) - I(U_1;U_2|Q) \ , \tag{4.152}$$
$$R_1 + R_2 \leq I(U_2;Y_2|Q) + I(QU_1;Y_1) - I(QU_1U_2;Z) - I(U_1;U_2|Q) \ , \tag{4.153}$$
$$R_1 + R_2 \leq I(QU_1;Y_1) + I(QU_2;Y_2) - I(QU_1U_2;Z) - I(U_1;U_2|Q) - I(Q;Z) \tag{4.154}$$

Obviously, the time sharing variable T can be added and thus, the achievability of the region (4.17) is proved. □

Summary

In this part of the work, we investigated the secrecy capacity region of the general memoryless two-user Wiretap Broadcast Channel.

We derived a novel outer bound which implies, to the best of our knowledge, all known capacity results in the corresponding setting while by removing secrecy constraints it performs as well as the best-known outer bound for the general Broadcast Channel. Despite a careful single letter derivations, we had to thoroughly analyse the role of auxiliary rvs in this outer bound, and thus could identify a set of auxiliary rvs that can be dropped when maximizing over a smaller set of constraints.

An inner bound on the secrecy capacity region of the WBC was also derived by resorting to existent encoding techniques based on random binning and stochastic encoders. The common and private auxiliary rvs of Marton's coding scheme are used to provide for secrecy jointly for both messages. The obtained inner bound recovers thus naturally Marton's inner bound for the BC when no secrecy is required.

The inner and outer bounds derived herein allowed us to characterize the secrecy capacity region of several classes of channels, including the deterministic BC with a general eavesdropper, the semi-deterministic BC with a more-noisy eavesdropper and the less-noisy BC with a degraded eavesdropper, as well as some classes of ordered BCs previously studied and the product of two inversely ordered BC with a degraded eavesdropper.

Furthermore, the secrecy capacities of the BC with BEC/BSC components and a BSC eavesdropper, was characterized relying on an inequality that is equivalent to Mrs Berger's Lemma extended to secrecy environments.

Conclusions and Perspectives

Conclusions and General comments

In this thesis, we investigated the interference mitigation for some Broadcast Networks.

We first investigated the general two-user Compound Broadcast Channel where an encoder wishes to transmit common and private messages to two receivers while being oblivious to two possible channel realizations controlling the communication. The focus was on the characterization of the largest achievable rate region by resorting to more evolved *encoding* and *decoding* techniques than the conventional coding for the standard BC. In Chapter 1, the role of the decoder was first explored, and an achievable rate region was derived based on the principle of Interference Decoding where each receiver decodes its intended message and chooses to (non-uniquely) decode or not the interfering message. This inner bound was shown to be capacity achieving for a class of relevant compound BEC/BSC broadcast channels while the worst-case of Marton's inner bound –based on Non Interference Decoding (NID)– fails to achieve the capacity region. Then, in Chapter 2, the role of the encoder was studied, and an achievable rate region was derived based on Multiple Description coding where the encoder transmits a common as well as multiple dedicated private descriptions to the many instances of the users channels. It turned out that MD coding outperforms the single description scheme –Common Description coding– for a class of compound MISO BC.

However we have to account here for some limitations inherent either to the model we were investigating or to the theoretic tools used to solve these problems. An important comment we can emit on the work we performed all along the first two chapters of this thesis, is that we relied on Marton's inner bound to derive inner bounds that would allow us to encompass as many capacity results as possible, it being the best inner bound hitherto known for the BC. With the application of Marton's coding and adapting it to the many settings we investigated, came the difficulty of evaluating the resulting inner bounds. Indeed, evaluating Marton's inner bound has long remained an open problem, and thus, called for consequent work to define bounds on the auxiliary variables alphabet [64], to define necessary conditions of the maximizing distributions [65], or even to bound the resulting sum rate for discrete input channels [66]. Other works dealt also with alternate formulations of Marton's inner bound [67] and [68] without however giving an easily maximized rate region.

Thus, when investigating the gain of ID in Compound BCs, besides the difficulty of identifying practical channels that would be relevant and yet would allow us to illustrate the strict gain over Marton's inner bound, we faced the very limitation of evaluating Marton's inner bound in the discrete example of BEC/BSC channel; a limitation that

we could alleviate by rather comparing ID to an outer bound on Marton's inner bound. However, when we proposed a more evolved encoding technique based on Multiple Description coding, which requires common and multiple dedicated private descriptions to the many instances of the users channels, we did not go in the direction of evaluating the whole Common Description inner bound, i.e Marton's inner bound, since the evaluation for continuous alphabets is even more challenging. Rather, we chose to compare two DPC coding schemes based on the two ideas of Common Description and Multiple Description coding, and upon carrying a thorough optimization of the CD-DPC inner bound, we could show that MD-DPC can strictly improve over the CD-DPC inner bound.

In Chapter 3 of this thesis, we investigated the Multicast Cognitive Interference Channel in an attempt to characterize the optimal strategy to apply when multiple primary users are interested in the same message. The results follow either from a straightforward extension of the known results in the no-Multicast case, or from rewriting new proofs – especially outer bounds– that can be extended to multiple users. It is thus implicit, that in the cases where the capacity region remains unknown for the CIFC, little could be done to characterize the multicast setting capacity region.

It seems but fair here to bring about the difficulty of writing inner bounds that could be the most general possible to combine superposition coding, random binning, and rate splitting. Such an inner bounding technique involves many auxiliary random variables, and thus many encoding and decoding constraints. Simplifying the resulting set of inequalities requires applying Fourier Motzkin Elimination which, in itself, prevents the processing of big number of inequalities. Thus a closed form of the inner bound is rather time-consuming if not infeasible in a reasonable time frame. However, maybe a very useful tool that one can resort to is the genie aided FME developed by Villard [69]. While most inner bounds in literature are not given in closed form [26], we chose to compute an inner bound that, though less general than [26], performs well enough to encompass many capacity results.

Finally, in Chapter 4 of the thesis, we investigated the secrecy capacity of the Wiretap Broadcast Channel with an external eavesdropper where a source wishes to communicate two private messages over a Broadcast Channel while keeping them secret from the eavesdropper. We derived a non-trivial outer bound on the secrecy capacity region of this channel which, in absence of security constraints, reduces to the best known outer bound to the capacity of the standard BC, i.e Nair & El Gamal outer bound. An inner bound was also derived which follows the behaviour of both the best known inner bound for the BC and the Wiretap Channel. These bounds were shown to be tight for some classes of Wiretap Broadcast Channels. We illustrated then our results by studying the impact of security constraints on the capacity of the WBC with BEC and BSC components.

In the same line of the long standing open problems we encountered in this work, we can cite also extending the model to the Wiretap Broadcast Channel with a common message. Indeed, transmitting a common message to two users while keeping it secret from an external eavesdropper is still an unsolved problem [70] [71]. Hence, we did only consider private message transmissions in the light of this underlying open problem.

Discussion and Future work

1 The Compound Broadcast Channel

We start our discussion with the analysis of the relative behavior of the MD and the ID inner bounds, to understand if there is any mutual inclusion between the two bounds. The question we want to answer is whether introducing multiple descriptions, one for each instance in the compound setting, allows to recover the ID inner bound. We also would like to understand to what extent decoding interference is crucial for Marton's worst case inner bound.

Can Multiple Descriptions or Interference Decoding recover one another?

For this sake, we evaluate the MD inner bound in the case of the discrete example studied in Section 1.2 and try to identify a set of auxiliary RVs yielding the capacity region. For the discrete Compound BC we studied earlier, we assumed that user 1 could observe one of two possible channel instances, namely, Y_1 and Y_2, such that Y_2 is more capable than both Y_1 and Z, and Y_1 be a degraded version of Z. The maximizing choice of auxiliary RVs led to Z and Y_2 decoding all the signal and Y_1 decoding only its intended information.

The capacity region is of the form:

$$\begin{cases} R_1 & \leq & I(Q;Y_1) \ , \\ R_1 + R_2 & \leq & I(Q;Y_1) + I(X;Z|Q) \ . \end{cases} \tag{1}$$

We next discuss a formulation of the MD inner bound that captures the intuition of the capacity achieving choice of auxiliary rv for ID inner bound. Indeed, the encoder does not transmit a common description to the two users interested in the same message, but communicates only private descriptions to them. However, in the present case, the common auxiliary rv Q is no longer a time-sharing variable as it was the case in Section 2.1, it can carry common information to all receivers as well. With this, we can achieve the set of rate pairs satisfying:

$$\mathcal{R}_{\text{3-ARV}} = \bigcup_{p_{QU_1U_2VX}} \left(\bigcup_{(T_{1,1},T_{1,2},T_2)\in\mathbb{T}(p)} \mathcal{M}(p, T_{1,1}, T_{1,2}, T_2) \right) \ , \tag{2}$$

where $\mathcal{M}$ and $\mathbb{T}$ are respectively defined by the following:

$$\mathcal{M}: \begin{cases} T_2 & \leq & I(V;Z|Q)\,, \\ R_0+T_2 & \leq & I(QV;Z)\,, \\ T_{1,1} & \leq & I(U_1;Y_1|Q)\,, \\ R_0+T_{1,1} & \leq & I(QU_1;Y_1)\,, \\ T_{1,2} & \leq & I(U_2;Y_2|Q)\,, \\ R_0+T_{1,2} & \leq & I(QU_2;Y_2)\,, \end{cases} \tag{3}$$

$$\mathbb{T} = \Big\{(T_{1,1},T_{1,2},T_2): \quad T_2 \geq R_2 \ ,\ \min\{T_{1,1},T_{1,2}\} \geq R_1\,, \tag{4}$$

$$T_{1,1} - R_1 + T_2 - R_2 > I(U_1;V|Q)\,, \tag{5}$$

$$T_{1,2} - R_1 + T_2 - R_2 > I(U_2;V|Q)\,, \tag{6}$$

$$T_{1,1} - R_1 + T_{1,2} - R_1 > I(U_1;U_2|Q)\,, \tag{7}$$

$$T_{1,1} + T_{1,2} - 2\,R_1 + T_2 - R_2 > I(U_1;U_2|Q) + I(U_1U_2;V|Q)\Big\}\,. \tag{8}$$

Proof: The proof is relegated to Appendix C.6. ∎

We know that an optimal transmission scheme to achieve the capacity region of the considered BEC/BSC requires both users Z and Y_2 to decode all messages while restricting the weaker user Y_1 to decode only the common message. Hence, we rely on this argument to build the straightforward extension of Marton's coding scheme, i.e., $V = U_2 = X$ and $U_1 = Q$, which along with rate splitting leads to the following achievable rate region:

$$\begin{cases} R_1 & \leq & I(Q;Y_1)\,, \\ R_1+R_2 & \leq & I(X;Z|Q) + I(X;Y_2|Q) + \min\{I(Q;Y_1), I(Q;Y_2)\} - H(X|Q)\,. \end{cases} \tag{9}$$

In the general case, there is strong evidence that the above rate region induced by MD is strictly included in the capacity region given by:

$$\begin{cases} R_1 & \leq & I(Q;Y_1)\,, \\ R_1+R_2 & \leq & I(X;Z|Q) + I(Q;Y_1)\,, \end{cases} \tag{10}$$

that is achieved by using ID, which yields:

$$\begin{cases} R_1 & \leq & I(Q;Y_1)\,, \\ R_1+R_2 & \leq & \min\{I(X;Z|Q), I(X;Y_2|Q)\} + I(Q;Y_1)\ , \\ R_1+R_2 & \leq & \min\{I(X;Z), I(X;Y_2)\}\ , \end{cases} \tag{11}$$

where Y_1 is degraded with respect to Z and Y_2 is more capable than Z. The inclusion results from the fact that there exist $P_{X|Q}$ for which

$$I(X;Y_2|Q) - H(X|Q) < 0\ . \tag{12}$$

Thus, MD does not seem to be enough to achieve the capacity region of the compound model investigated in Section 1.2. This is due to the fact that the cost engendered by precoding against interference prevents from decoding it which results in a loss proportional to its entropy. Therefore, it appears that ID outperforms MD in some cases.

On the other hand, in the MISO case, imposing on users to decode interference is sub-optimal, at least from a DoF perspective, since ID introduces sum-rates constraints of the form

$$R_1 + R_2 \leq I(X; Y_1) \ , \tag{13}$$

and thus, prevents the sum-DoF from reaching values greater than 1 which we already know is sub-optimal. Therefore, it is crucial to precode against interference.

Summarizing, since neither MD coding or ID seem to generalize all the results obtained herein one can benefit from the combination of both techniques and thus, from the optimization of both encoding and decoding schemes. This constitutes an interesting way to investigate on.

It is our belief that, among the theoretic aspects that have yet to be explored, many capacity results for the Compound Broadcast Channel can be found provided new outer bounds are derived for such settings. It is thus crucial that more research be dedicated to this problem.

2 The Multicast Cognitive Interference Channel

As for the Multicast Cognitive Interference Channel, the best way to investigate seems to be the "better cognitive decoding" regime. In the non-mutlicast setting, this regime is defined by

$$I(UX_1; Y) \leq I(UX_1; Z) \ , \tag{14}$$

for all auxiliary rv U satisfying $U \multimap (X_1, X_2) \multimap (Y, Z)$, and its capacity region is given by the set of rate pairs satisfying:

$$\begin{cases} R_1 & \leq & I(UX_1; Y) \ , \\ R_2 & \leq & I(X_2; Z|X_1) \ , \\ R_1 + R_2 & \leq & I(UX_1; Y) + I(X_2; Z|UX_1) \ . \end{cases} \tag{15}$$

The extension of such a regime, would imply having for all users, in the multicast set, indexed by $j \in [1 : N]$,

$$I(UX_1; Y_j) \leq I(UX_1; Z) \ . \tag{16}$$

The challenging issue in this case is the outer bounding technique that involves inevitably Csiszár & Körner's sum identity, which we know can not be extended to arbitrary number of users. Thus, one could think of writing a new outer bound that would not rely on such a sum identity, similarly to what we did in the weak interference case, and thus the extension to the mutlicast setting would follow in a straightforward manner.

Since in this work we evaluated the capacity of some Gaussian regimes, we did not however characterize the capacity of all settings for which capacity is known, namely the "S-CIFC" and the "primary decodes cognitive" regimes [45], in the multicast extension. This could also form the agenda of future work in this case.

3 The Wiretap Broadcast Channel

In the last part of this thesis, we investigated the BC with secrecy constraints, namely, the Wiretap Broadcast Channel. In such a setting, in an attempt to characterize the secrecy capacity region, we had to resort to a non-trivial equivalent formulation of our outer bound by showing that a set of auxiliaries was unnecessary to the maximization of the outer bound.

In the same spirit of Corollary 35, a more general study of the role of the auxiliary variables of the outer bound in Theorem 35 may lead to the characterization of capacity for other classes of Wiretap BCs and this will be object of future work. Such an approach can also be extended to other channels and it is our belief that by analysing the role of auxiliaries, one can recover the capacity of many classes of Wiretap Broadcast networks, e.g alleviating constraints of less-noisiness among the legitimate user and the eavesdropper in the Less-noisy BC with a partly degrade eavesdropper.

Another horizon of investigation is the introduction of a common shared message, that needs not be secure towards the eavesdropper. Again, with the new upper bounding techniques we could develop, we might be able to recover the capacity region of some settings. In a first attempt to solve such a problem, we could write the two following outer bound:

$$R_0 \leq \min\{I(TV_1;Y_1), I(TV_2;Y_2)\} \ , \tag{17}$$
$$R_1 \leq I(U_1;Y_1|TV_1) - I(U_1;Z|TV_1) \ , \tag{18}$$
$$R_2 \leq I(U_2;Y_2|TV_2) - I(U_2;Z|TV_2) \ , \tag{19}$$
$$R_1 + R_2 \leq I(X;Y_1|U_2TZV_2) + I(U_2;Y_2|TV_2) - I(U_2;Z|TV_2) \ , \tag{20}$$
$$R_1 + R_2 \leq I(X;Y_2|U_1TZV_1) + I(U_1;Y_1|TV_1) - I(U_1;Z|TV_1) \ , \tag{21}$$

where $TU_1V_1U_2V_2$ are arbitrarily correlated.

On the other side, an inner bound we could write consists in:

$$R_0 \leq \min\{I(T,Y_1), I(T;Y_2)\} \ , \tag{22}$$
$$R_1 \leq I(QU_1;Y_1|T) - I(QU_1;Z|T) \ , \tag{23}$$
$$R_2 \leq I(QU_2;Y_2|T) - I(QU_2;Z|T) \ , \tag{24}$$
$$\begin{aligned} R_1 + R_2 \leq \min\Big\{ & I(Q;Y_1|T) \ , \ I(Q;Y_2|T) \ , \ I(Q;Y_1|T) + I(Q;Y_2|T) - I(Q;Z|T) \Big\} \\ & + I(U_1;Y_1|TQ) + I(U_2;Y_2|TQ) - I(QU_1U_2;Z|T) - I(U_1;U_2|QT) \ . \end{aligned} \tag{25}$$

It would be interesting to identify classes of WBCs for which these two bounds are tight, this also forms agenda of future work.

Appendices

Appendix A

Useful Notions and Results

The appendix below provides basic notions on some concepts used in this thesis.

Following [72], we use in this thesis *strongly typical sets* and the so-called *Delta-Convention*. Some useful facts are recalled here. Let X and Y be rvs on some finite sets $\mathcal{X}$ and $\mathcal{Y}$, respectively. We denote by P_{XY} (resp. $P_{Y|X}$, and P_X) the joint probability distribution of (X,Y) (resp. conditional distribution of Y given X, and marginal distribution of X).

Definition 44. *For any sequence $x^n \in \mathcal{X}^n$ and any symbol $a \in \mathcal{X}$, notation $N(a|x^n)$ stands for the number of occurrences of a in x^n.*

Definition 45. *A sequence $x^n \in \mathcal{X}^n$ is called* (strongly) δ-typical *w.r.t. X (or simply* typical *if the context is clear) if*

$$\left|\frac{1}{n}N(a|x^n) - P_X(a)\right| \leq \delta \quad \textit{for each } a \in \mathcal{X} \ ,$$

and $N(a|x^n) = 0$ for each $a \in \mathcal{X}$ such that $P_X(a) = 0$. The set of all such sequences is denoted by $T_\delta^n(X)$.

Definition 46. *Let $x^n \in \mathcal{X}^n$. A sequence $y^n \in \mathcal{Y}^n$ is called* (strongly) δ-typical (w.r.t. Y) given x^n *if*

$$\left|\frac{1}{n}N(a,b|x^n,y^n) - \frac{1}{n}N(a|x^n)P_{Y|X}(b|a)\right| \leq \delta \quad \textit{for each } a \in \mathcal{X}, b \in \mathcal{Y} \ ,$$

and, $N(a,b|x^n,y^n) = 0$ for each $a \in \mathcal{X}$, $b \in \mathcal{Y}$ such that $P_{Y|X}(b|a) = 0$. The set of all such sequences is denoted by $T_\delta^n(Y|x^n)$.

Delta-Convention [72]: For any sets $\mathcal{X}$, $\mathcal{Y}$, there exists a sequence $\{\delta_n\}_{n\in\mathbb{N}^*}$ such that lemmas below hold.[7] From now on, typical sequences are understood with $\delta = \delta_n$. Typical sets are still denoted by $T_\delta^n(\cdot)$.

Lemma 5 ([72, Lemma 1.2.12])**.** *There exists a sequence $\eta_n \xrightarrow[n\to\infty]{} 0$ such that*

$$P_X^n(T_\delta^n(X)) \geq 1 - \eta_n \ .$$

[7] As a matter of fact, $\delta_n \to 0$ and $\sqrt{n}\,\delta_n \to \infty$ as $n \to \infty$.

Lemma 6 ([72, Lemma 1.2.13])**.** *There exists a sequence* $\eta_n \xrightarrow[n\to\infty]{} 0$ *such that, for each* $x^n \in T_\delta^n(X)$*,*

$$\left|\frac{1}{n}\log\|T_\delta^n(X)\| - H(X)\right| \leq \eta_n \ ,$$
$$\left|\frac{1}{n}\log\|T_\delta^n(Y|x^n)\| - H(Y|X)\right| \leq \eta_n \ .$$

Lemma 7 (Asymptotic equipartition property)**.** *There exists a sequence* $\eta_n \xrightarrow[n\to\infty]{} 0$ *such that, for each* $x^n \in T_\delta^n(X)$ *and each* $y^n \in T_\delta^n(Y|x^n)$*,*

$$\left|-\frac{1}{n}\log P_X^n(x^n) - H(X)\right| \leq \eta_n \ ,$$
$$\left|-\frac{1}{n}\log P_{Y|X}^n(y^n|x^n) - H(Y|X)\right| \leq \eta_n \ .$$

Lemma 8 (Joint typicality lemma [63])**.** *There exists a sequence* $\eta_n \xrightarrow[n\to\infty]{} 0$ *such that*

$$\left|-\frac{1}{n}\log P_Y^n(T_\delta^n(Y|x^n)) - I(X;Y)\right| \leq \eta_n \quad \textit{for each } x^n \in T_\delta^n(X) \ .$$

Proof:

$$\begin{aligned} P_Y^n(T_\delta^n(Y|x^n)) &= \sum_{y^n \in T_\delta^n(Y|x^n)} P_Y^n(y^n) \\ &\overset{(a)}{\leq} \|T_\delta^n(Y|x^n)\|\, 2^{-n[H(Y)-\alpha_n]} \\ &\overset{(b)}{\leq} 2^{n[H(Y|X)+\beta_n]}\, 2^{-n[H(Y)-\alpha_n]} \\ &= 2^{-n[I(X;Y)-\beta_n-\alpha_n]} \ , \end{aligned}$$

where

- step (a) follows from the fact that $T_\delta^n(Y|x^n) \subset T_\delta^n(Y)$ and Lemma 7, for some sequence $\alpha_n \xrightarrow[n\to\infty]{} 0$,
- step (b) from Lemma 6, for some sequence $\beta_n \xrightarrow[n\to\infty]{} 0$.

The reverse inequality $P_Y^n(T_\delta^n(Y|x^n)) \geq 2^{-n[I(X;Y)+\beta_n+\alpha_n]}$ can be proved following similar argument. ■

Lemma 9 (Csiszár & Körner's sum-identity [21, Lemma 7])**.** *Consider two i.i.d. sequences* X^n *and* Y^n*, and a constant* C*. The following identity holds:*

$$\sum_{i=1}^{n} I(Y_{i+1}^n; X_i|CX^{i-1}) = \sum_{j=1}^{n} I(X^{j-1}; Y_j|CY_{j+1}^n) \ . \tag{A.1}$$

Proof: From the chain rule for conditional mutual information, we can write:

$$\begin{aligned}\sum_{i=1}^{n} I(Y_{i+1}^{n}; X_i|CX^{i-1}) &= \sum_{i=1}^{n}\sum_{j=i+1}^{n} I(Y_j; X_i|CX^{i-1}Y_{j+1}^{n}) \\ &= \sum_{i,j:\ i<j} I(Y_j; X_i|CX^{i-1}Y_{j+1}^{n}) \\ &= \sum_{j=1}^{n}\sum_{i=1}^{j-1} I(X_i; Y_j|CX^{i-1}Y_{j+1}^{n}) \\ &= \sum_{j=1}^{n} I(X^{j-1}; Y_j|CY_{j+1}^{n}) \ .\end{aligned}$$

■

Appendix B

Proof of results of Chapter 1

B.1 Sketch of the Proof of Theorem 17

Let $j \in \mathcal{J}$ be the index of an arbitrary pair of users in the compound set. We first show the achievability of the union of the four regions for this channel $\bigcup_{i\in[1:4]} \mathcal{T}_i$. For convenience of notations we drop the index j.

B.1.1 Outline of Proof

The coding scheme we use is as follows:

- We use three auxiliary RVs, one for each message,
- We perform binning on the two auxiliary RV that code for the private messages, superposing them over the auxiliary RV coding for the common message,
- The decoding will introduce the principle of list decoding, which will allow us to combine two decoding techniques,
- The error probability will be shown to be directly related to the list size, and thus, bounding the list size will allow us to have a tight bound on the average probability of error,
- The intersection of the union of the regions comes from the fact that we use two different decoding functions at the two users.

B.1.2 Detailed Proof

Codebook generation: The encoding is similar to that of Marton's coding with a common message.

Fix, $P_Q, P_{U|Q}, P_{V|Q}$ and let $T_1 \geq R_1$ and $T_2 \geq R_2$ be four positive rates.

Generate 2^{nR_0} n-sequences $q^n(w_0), w_0 \in \mathcal{M}_0$ following each the probability distribution:

$$P_Q^n(w_0) = \prod_{i=1}^{n} P_Q(q_i(w_0)) \ , \tag{B.1}$$

and set them all in $\mathcal{C}_0$.

For each $q^n(w_0)$, generate 2^{nT_1} n-sequences $u^n(l_1, w_0)$, $l_1 \in [1 : 2^{nT_1}]$ each following

$$P_{U|Q}^n(u^n(l_1, w_0)) = \prod_{i=1}^{n} P_{U|Q}(u_i(l_1, w_0)|q_i(w_0)) \ , \tag{B.2}$$

and map all these sequences in 2^{nR_1} bins, each indexed with $w_1 \in [1 : 2^{nR_1}]$: $\mathcal{C}(w_1, w_0)$.

Generate similarly 2^{nT_2} n-sequences $v^n(l_2, w_0)$, $l_2 \in [1 : 2^{nT_2}]$ each following $P_{V|Q}^n(v^n(l_2, w_0))$ and map them into 2^{nR_2} bins: $\mathcal{C}(w_2, w_0)$.

Encoding:

To send a message vector: (W_0, W_1, W_2), the encoder first finds a pair of sequences $(u^n(L_1, W_0), v^n(L_2, W_0))$ in the product bins $\mathcal{C}(W_j, W_0)$ such that:

$$\Big(q^n(W_0), u^n(L_1, W_0), v^n(L_2, W_0)\Big) \in T_\delta^n(QUV) \ , \tag{B.3}$$

and then transmits: $x^n\Big(q^n(W_0), u^n(L_1, W_0), v^n(L_2, W_0)\Big)$ which is generated via a random mapping.

Decoding:

First, assume that no " encoding error: ϵ_0" has occurred, and note: (L_1, L_2) the chosen indices. For a matter of conciseness, we consider only Decoder 1.

Given a received sequence y^n, define the two lists:

$$\mathcal{L}_1(y^n) \triangleq \Big\{(w_0, w_1) \,\Big|\, (q^n(w_0), u^n(l_1, w_0), y^n) \in T_\delta^n(QUY) \text{ for } u^n(l_1, w_0) \in \mathcal{C}(w_1, w_0)\Big\} \tag{B.4}$$

$$\mathcal{L}_2(y^n) \triangleq \Big\{(w_0, w_1) \,\Big|\, (q^n(w_0), u^n(l_1, w_0), v^n(l_2, w_0), y^n) \in T_\delta^n(QUVY)$$
$$\text{for some } w_2 \,,\ v^n(l_2, w_0) \in \mathcal{C}(w_2, w_0) \,,\ \text{ and } u^n(l_1, w_0) \in \mathcal{C}(w_1, w_0))\Big\}. \tag{B.5}$$

These lists correspond to two different decoding functions: "non-unique" decoding of the other user's message, and "not" decoding it. Denote the intersection of these two lists by

$$\mathcal{L}^{(n)} \triangleq \mathcal{L}_1(y^n) \cap \mathcal{L}_2(y^n). \tag{B.6}$$

Analysis of the probability of error: To analyze the probability of error at user 1, we need to control the expected cardinality of the intersection of the above lists. The next lemma (shown in Appendix B.2) states this result.

Lemma 10. *For every $\epsilon_1 > 0$, the average probability of error is linked to the list size as follows:*

$$P_e^{(n)} \leq \mathbb{P}\{\|\mathcal{L}^{(n)}\| \geq 2\} + \epsilon_1 \tag{B.7}$$

for $n > \exists\, N_1$ large enough.

Now, bounding the probability of error will mainly consist in bounding the decoding list size.

Bounding the list size:

On one hand, the list size being an integer valued RV, we can write:

$$\mathbb{P}\{\|\mathcal{L}^{(n)}\| \geq 2\} \leq \mathbb{E}[\|\mathcal{L}^{(n)}\|] - \mathbb{P}\{\|\mathcal{L}^{(n)}\| \geq 1\}. \tag{B.8}$$

On the other hand:

$$\mathbb{E}\|\mathcal{L}^{(n)}\| = \mathbb{P}\{(W_0, W_1) \in \mathcal{L}^{(n)}\} + \sum_{(w_0,w_1)\neq(W_0,W_1)} \mathbb{P}\{(w_0, w_1) \in \mathcal{L}^{(n)}\}. \tag{B.9}$$

The next lemma provides a bound on the expected list size from the RHS of (B.9). The proof is relegated to Appendix B.2.

Lemma 11 (Bounding the probability of undetected errors)**.** *The probability of decoding $(w_0, w_1) \neq (W_0, W_1)$, can be upper-bounded as follows:*

$$\sum_{(w_0,w_1)\neq(W_0,W_1)} \mathbb{P}\{(w_0, w_1) \in \mathcal{L}^{(n)}\} \leq \min\{I_1^{(n)}, I_2^{(n)}\} \ , \tag{B.10}$$

for n large enough, i.e. $n > N_2$, for some N_2, where:

$$I_1^{(n)} \triangleq \exp_2\Big(n\left[T_1 - I(U;Y|Q) + \epsilon_2\right]\Big) + \exp_2\Big(n\left[R_0 + T_1 - I(QU;Y) + \epsilon_2\right]\Big) \ , \tag{B.11}$$

$$I_2^{(n)} \triangleq \exp_2\Big(n\left[T_1 - I(U;YV|Q) + \epsilon_3\right]\Big) + \exp_2\Big(n\left[T_1 + T_2 - I(UV;Y|Q) - I(U;V|Q) + \epsilon_3\right]\Big) + \exp_2\Big(n\left[R_0 + T_1 + T_2 - I(QUV;Y) - I(U;V|Q) + \epsilon_3\right]\Big). \tag{B.12}$$

Hence, from (B.8), (B.9) and (B.10) we can write that:

$$\mathbb{P}\{\|\mathcal{L}^{(n)}\| \geq 2\} \leq \min\{I_1^{(n)}, I_2^{(n)}\} \ . \tag{B.13}$$

Then Lemma 1 and (B.13), imply that for n large enough:

$$P_e^{(n)} \leq \mathbb{P}\{\|\mathcal{L}^{(n)}\| \geq 2\} + \epsilon_1 \leq \min\{I_1^{(n)}; I_2^{(n)}\} + \epsilon_1 \ . \tag{B.14}$$

Thus, provided that:

$$\limsup_{n\to\infty} \min\{I_1^{(n)}, I_2^{(n)}\} = 0 \ , \tag{B.15}$$

the probability of error at user 1, knowing that no encoding error occurred, will tend to 0 as $n \to \infty$.

Following the proof of the Covering lemma [63], the probability of encoding error can be upper bounded as n grows large enough as follows:

$$\mathbb{P}(\epsilon_0) \leq \exp_2\Big(n\left[I(U;V|Q) - (T_1 - R_1 + T_2 - R_2) + \epsilon'\right]\Big). \tag{B.16}$$

The condition for no such error does not depend on the users pair index, and thus, it intersects the union of all regions, which concludes the proof.

B.2 The probability of error is linked to list size

Proof of Lemma 10

Let us start by recalling:

$$\mathcal{L}_1(Y^n) \cap \mathcal{L}_2(Y^n) = \mathcal{L}^{(n)}. \tag{B.17}$$

Let $(\hat{W}_0, \hat{W}_1)$ be the estimated messages at decoder 1, where

$$\begin{aligned}
&\mathbb{P}\{(\hat{W}_0, \hat{W}_1) \neq (W_0, W_1)\} \\
&= \delta \mathbb{P}\{\exists (\hat{w_0}, \hat{w_1}) \neq (W_0, W_1) \,:\, (\hat{w_0}, \hat{w_1}) \in \mathcal{L}^{(n)} | (W_0, W_1) \in \mathcal{L}^{(n)}\} + \\
&(1-\delta)\mathbb{P}\{\exists (\hat{w_0}, \hat{w_1}) \neq (W_0, W_1) \,:\, (\hat{w_0}, \hat{w_1}) \in \mathcal{L}^{(n)} | (W_0, W_1) \notin \mathcal{L}^{(n)}\} \qquad \text{(B.18)} \\
&\leq \mathbb{P}\{\|\mathcal{L}^{(n)}\| > 1\} + (1-\delta) \;, \qquad \text{(B.19)}
\end{aligned}$$

with $(1-\delta) \triangleq \mathbb{P}\{(W_0, W_1) \notin \mathcal{L}^{(n)}\}$.

Then, following standard arguments, by the LLN and independence of codebooks, we can easily show that, for all $\epsilon_1 > 0$, $\exists\, N_1$ such that for $n \geq N_1$, we have $(1-\delta) \leq \epsilon_1$.

This ends the proof of the statement:

$$P_e^{(n)} \leq \mathbb{P}\{\|\mathcal{L}^{(n)}\| \geq 2\} + \epsilon_1 \;. \qquad \text{(B.20)}$$

Proof of Lemma 11

Let $(w_0, w_1) \neq (W_0, W_1)$ be the supposedly decoded pair of messages. We have, recalling (B.6), that:

$$\mathbb{P}\{(w_0, w_1) \in \mathcal{L}^{(n)}\} \leq \min_{j=1,2} \mathbb{P}\{(w_0, w_1) \in \mathcal{L}_j(Y^n)\} \;. \qquad \text{(B.21)}$$

For the first list, we have, following similar arguments of Lemma 8, that:

$$\begin{aligned}
\mathbb{P}\{(W_0, w_1) \in \mathcal{L}_1(Y^n)\} &= \mathbb{P}\{(q^n(w_0), u^n(l_1, w_0), y^n) \in T_\delta^n(QUY) \text{ for } l_1 \in [1 : 2^{n(T_1 - R_1)}]\} \qquad \text{(B.22)} \\
&\leq \sum_{l_1 \in [1:2^{n(T_1-R_1)}]} \mathbb{P}\{(q^n(w_0), u^n(l_1, w_0), y^n) \in T_\delta^n(QUY)\} \qquad \text{(B.23)} \\
&\leq \exp_2\Big(n\left[T_1 - R_1 - I(U;Y|Q) + \epsilon_2\right]\Big) \;, \qquad \text{(B.24)}
\end{aligned}$$

and similarly, if moreover $w_0 \neq W_0$,

$$\mathbb{P}\{(w_0, w_1) \in \mathcal{L}_1(Y^n)\} \leq \exp_2\Big(n\left[T_1 - R_1 - I(QU;Y) + \epsilon_2\right]\Big) \;. \qquad \text{(B.25)}$$

Now, for the second list, i.e, decoding method, we know that:
1) If $w_0 = W_0$, $w_1 \neq W_1$ and $l_2 = L_2$ which implies $w_2 = W_2$:

$$\begin{aligned}
&\mathbb{P}\Big\{(Q^n(W_0), U^n(l_1, W_0), V^n(L_2, W_0), Y^n) \in T_\delta^n(QUVY) \text{ for } l_1 \in [1 : 2^{n(T_1-R_1)}]\Big\} \\
&\leq \exp_2\Big(n\left[T_1 - R_1 + H(QUVY) - H(Q) - H(U|Q) - H(YV|Q) + \epsilon_3\right]\Big) \qquad \text{(B.26)} \\
&= \exp_2\Big(n\left[T_1 - R_1 - I(U;YV|Q) + \epsilon_3\right]\Big) \;, \qquad \text{(B.27)}
\end{aligned}$$

where we used the fact that, since $w_1 \neq W_1$, then $U^n(l_1, W_0)$ and $V^n(L_2, W_0)$ are independent conditionally on $Q^n(W_0)$.
2) If $w_0 = W_0$, $w_1 \neq W_1$, and $l_2 \neq L_2$ then:

$$\begin{aligned}
&\mathbb{P}\Big\{(Q^n(W_0), U^n(l_1, W_0), V^n(l_2, W_0), Y^n) \in T_\delta^n(QUVY) \text{ for } l_1 \in [1 : 2^{n(T_1-R_1)}]\Big\} \\
&\leq \exp_2\Big(n\left[T_1 - R_1 + H(QUVY) - H(Q) - H(U|Q) - H(V|Q) - H(Y|Q) + \epsilon_3\right]\Big) \qquad \text{(B.28)} \\
&= \exp_2\Big(n\left[T_1 - R_1 - I(UV;Y|Q) - I(U;V|Q) + \epsilon_3\right]\Big) \;. \qquad \text{(B.29)}
\end{aligned}$$

3) Finally, if $w_0 \neq W_0$, then whatever l_1 and l_2:

$$\begin{aligned} &\mathbb{P}\Big\{(Q^n(w_0), U^n(l_1, w_0), V^n(l_2, w_0), Y^n) \in T_\delta^n(QUVY)\Big\} \\ &\leq \exp_2\Big(n\left[H(QUVY) - H(Q) - H(U|Q) - H(V|Q) - H(Y) + \epsilon_3\right]\Big) \qquad \text{(B.30)} \\ &= \exp_2\Big(n\left[-I(QUV;Y) - I(U;V|Q) + \epsilon_3\right]\Big)\ . \qquad \text{(B.31)} \end{aligned}$$

This ends the proof of Lemma 2.

B.3 Outer Bound Derivation for the Compound BC

We need to recall that the proof in [28] of the outer bound for users' pair (k), uses the specific choice of auxiliary RV:

$$\left\{\begin{array}{rcl} U_i & = & W_1\ , \\ V_i & = & W_2\ , \\ Q_i^{(k)} & = & (Y^{i-1,(k)}, Z_{i+1}^{n,(k)})\ . \end{array}\right. \qquad \text{(B.32)}$$

Here, we notice that the auxiliary RV (U_i, V_i) do not the depend on the users' pair index. Thus, we can show that for all channel indices (k) with the specific choice: $U_i = W_1$, $V_i = W_2$,

$$\mathcal{R}_{\text{NEG}}^{(k)}(p_{QUVX}) : \left\{\begin{array}{rcl} nR_1 & \leq & \sum_{i=1}^{n} I(Q_{k,i}U_i; Y_{k,i})\ , \\ nR_2 & \leq & \sum_{i=1}^{n} I(Q_{k,i}V_i; Z_{k,i})\ , \\ n(R_1+R_2) & \leq & \sum_{i=1}^{n} \Big[I(U_i; Y_{k,i}|Q_{k,i}V_i) + I(Q_{k,i}V_i; Z_{k,i})\Big]\ , \\ n(R_1+R_2) & \leq & \sum_{i=1}^{n} \Big[I(Q_{k,i}U_i; Y_{k,i}) + I(V_i; Z_{k,i}|Q_{k,i}U_i)\Big]\ , \end{array}\right. \qquad \text{(B.33)}$$

where $Q_{k,i} = (Y_{k,1}^{i-1}, Z_{k,i+1}^{n})$. Thus, we could possibly factor the resulting joint pmf on (U_i, V_i) over all compound channel indices, and let only the common variable choice vary from one channel to another. Moreover, we can show in the same fashion as in [28, Lemma 3.2], that the maximizing distribution of the input $p_{X|QUV}$ is a deterministic mapping.

B.4 Proof of Achievability of the Capacity

From Theorem 17, we can see that the region $\mathcal{R}_{\text{SNID}}$ verifies:

$$\mathcal{R}_{\text{SNID}} \supseteq \bigcup_{p_{QUVX}\in\mathcal{P}} \bigcup_{(T_1,T_2)\in\mathbb{T}(p)} \Big(\mathcal{T}_3^{(1)}(p, T_1, T_2) \cap \mathcal{T}_4^{(2)}(p, T_1, T_2)\Big)\ , \qquad \text{(B.34)}$$

In this section, we evaluate the region thus obtained by:

$$\mathcal{R}_{\text{SNID}}^{\star} \triangleq \bigcup_{p_{QUVX}\in\mathcal{P}} \bigcup_{(T_1,T_2)\in\mathbb{T}(p)} \Big(\mathcal{T}_3^{(1)}(p, T_1, T_2) \cap \mathcal{T}_4^{(2)}(p, T_1, T_2)\Big)\ , \qquad \text{(B.35)}$$

where $\mathcal{T}_3^{(1)} \cap \mathcal{T}_4^{(2)}$ is the subset of $\Re_+^2$ defined by the inequalities:

$$\left\{\begin{array}{rcl} T_2 & \leq & I(V;ZU|Q) \\ T_1+T_2 & \leq & I(UV;Z|Q)+I(U;V|Q) \\ R_0+T_1+T_2 & \leq & I(QUV;Z)+I(U;V|Q) \\ T_1 & \leq & I(U;Y_2V|Q) \\ T_1+T_2 & \leq & I(UV;Y_2|Q)+I(U;V|Q) \\ R_0+T_1+T_2 & \leq & I(QUV;Y_2)+I(U;V|Q) \\ T_1 & \leq & I(U;Y_1|Q) \\ R_0+T_1 & \leq & I(QU;Y_1) \\ T_1 \geq R_1 & , & T_2 \geq R_2\,, \\ T_1+T_2 & > & R_1+R_2+I(U;V|Q) \end{array}\right. \tag{B.36}$$

Recalling here that Y_1 is physically degraded towards Z, we can first rewrite the decoding constraints as the following:

$$\left\{\begin{array}{rcl} T_2 & \leq & I(V;ZU|Q) \\ T_1 & \leq & \min\{I(U;Y_1|Q), I(U;Y_2V|Q)\} \\ R_0+T_1 & \leq & I(QU;Y_1) \\ T_1+T_2 & \leq & I(UV;Y_2|Q)+I(U;V|Q) \\ R_0+T_1+T_2 & \leq & I(QUV;Y_2)+I(U;V|Q)\ . \end{array}\right. \tag{B.37}$$

The, we can run FME over the binning rate pair $(T_1, T2)$ to get the following region:

$$\left\{\begin{array}{rcl} R_2 & \leq & I(V;ZU|Q) \\ R_1 & \leq & \min\{I(U;Y_1|Q), I(U;Y_2V|Q)\} \\ R_0+R_1 & \leq & I(QU;Y_1) \\ R_1+R_2 & \leq & I(UV;Y_2|Q) \\ R_1+R_2 & \leq & I(V;Z|UQ)+\min\{I(U;Y_1|Q), I(U;Y_2V|Q)\} \\ R_0+R_1+R_2 & \leq & I(QUV;Y_2) \\ R_0+R_1+R_2 & \leq & I(V;Z|UQ)+I(QU;Y_1)\ . \end{array}\right. \tag{B.38}$$

Later, we chose to apply *bit recombination* on the admissible rates (R_0, R_1, R_2) as follows:

$$\left\{\begin{array}{rcl} R_0 & = & R_0^\star + R_{01}^\star + R_{02}^\star\ , \\ R_1 & = & R_1^\star - R_{01}^\star \geq 0\ , \\ R_2 & = & R_2^\star - R_{02}^\star \geq 0\ , \\ R_{01}^\star & \geq 0 & ,\ R_{02}^\star \geq 0\ . \end{array}\right. \tag{B.39}$$

It is straightforward that this bit recombination fits the decoding logic of the terminals, i.e., part of the private messages is mapped into the common message, enabling each

terminal to still recover the totality of its intended message. The region writes thus as:

$$\begin{cases} R_2^\star - R_{02}^\star \leq I(V;ZU|Q) \\ R_1^\star - R_{01}^\star \leq \min\{I(U;Y_1|Q), I(U;Y_2V|Q)\} \\ R_0^\star + R_1^\star + R_{02}^\star \leq I(QU;Y_1) \\ R_1^\star - R_{01}^\star + R_2^\star - R_{02}^\star \leq I(UV;Y_2|Q) \\ R_1^\star - R_{01}^\star + R_2^\star - R_{02}^\star \leq I(V;Z|UQ) + \min\{I(U;Y_1|Q), I(U;Y_2V|Q)\} \\ R_0^\star + R_1^\star + R_2^\star \leq I(QUV;Y_2) \\ R_0^\star + R_1^\star + R_2^\star \leq I(V;Z|UQ) + I(QU;Y_1) \\ R_1^\star \geq R_{01}^\star \ , \ R_2^\star \geq R_{02}^\star \quad , \quad R_{01}^\star \geq 0 \ , \ R_{02}^\star \geq 0 \end{cases} \tag{B.40}$$

Performing again FME over the splitting rate pair $(R_{01}^\star, R_{02}^\star)$, we get the following region:

$$\begin{aligned} R_0^\star + R_1^\star &\leq I(QU;Y_1) \\ R_0^\star + R_1^\star + R_2^\star &\leq I(QU;Y_1) + I(UV;Y_2|Q) \\ R_0^\star + R_1^\star + R_2^\star &\leq I(QU;Y_1) + I(V;ZU|Q) && \text{(B.41)} \\ R_0^\star + R_1^\star + R_2^\star &\leq I(QU;Y_1) + I(V;Z|UQ) + \min\{I(U;Y_1|Q), I(U;Y_2V|Q)\} && \text{(B.42)} \\ R_0^\star + R_1^\star + R_2^\star &\leq I(QUV;Y_2) \\ R_0^\star + R_1^\star + R_2^\star &\leq I(U;Y|VQ) + I(QU;Y_1) \ . && \text{(B.43)} \end{aligned}$$

We clearly notice that the constraints: (B.41) and (B.42) are implied by (B.43), thus, the resulting region $\mathcal{R}_{\text{SNID}}^\star$ is defined by the following constraints:

$$\begin{cases} R_0^\star + R_1^\star \leq I(QU;Y_1) \\ R_0^\star + R_1^\star + R_2^\star \leq I(QU;Y_1) + I(UV;Y_2|Q) \\ R_0^\star + R_1^\star + R_2^\star \leq I(QUV;Y_2) \\ R_0^\star + R_1^\star + R_2^\star \leq I(V;Z|UQ) + I(QU;Y_1) \ . \end{cases} \tag{B.44}$$

Thus, letting $R_0^\star = 0$, and noting the rate pairs as (R_1, R_2), one gets the desired rate region.

B.5 Cardinality bounds

Consider a pair of RVs (Q, X) following the joint probability distribution $p_Q p_{X|Q}$. Since the input is binary, let the four continuous functions on $P_{X|Q}$:

$$f_1\Big(P_{X|Q}(0|q)\Big) = P_{X|Q}(0|q) \ , \tag{B.45}$$

$$f_2\Big(P_{X|Q}(0|q)\Big) = H(Z|Q=q) = H_2(p \star P_{X|Q}(0|q)) \ , \tag{B.46}$$

$$f_3\Big(P_{X|Q}(0|q)\Big) = H(Y_1|Q=q) = H_2(p_1 \star P_{X|Q}(0|q)) \ , \tag{B.47}$$

$$f_4\Big(P_{X|Q}(0|q)\Big) = H(X|Q=q) = H_2(P_{X|Q}(0|q)) \ . \tag{B.48}$$

By the usual consequence of Fenchel-Eggleston-Caratheodory theorem [72], we can construct an auxiliary RV Q' such that:

$$\sum_q P_Q(q) P_{X|Q}(0|q) = \sum_{q'} P_{Q'}(q') P_{X|Q}(0|q') = P_X(0) \ , \tag{B.49}$$

$$H(Z|Q)=H(Z|Q') \ , \tag{B.50}$$
$$H(Y_1|Q)=H(Y_1|Q') \ , \tag{B.51}$$
$$H(X|Q)=H(X|Q') \ , \tag{B.52}$$
$$\|Q'\|\leq 4 \ . \tag{B.53}$$

Thus, we conclude that with this new auxiliary RV Q', the region is unchanged:

$$I(X;Z|Q)=H(Z|Q) - H(Z|X) = H(Z|Q') - H_2(p) = I(X;Z|Q') \ , \tag{B.54}$$
$$I(Q;Y_1)=H(Y_1) - H(Y_1|Q) = H_2\left(p_1 \star P_X(0)\right) - H(Y_1|Q') = I(Q';Y_1) \ , \tag{B.55}$$
$$I(Q;Y_2)=(1-e)\left(H(X) - H(X|Q)\right) = \bar{e}\left(H_2(P_X(0)) - H(X|Q')\right) = I(Q';Y_2) \tag{B.56}$$

Input uniformity

In [29] lies a definition of the "c-symmetric broadcast channel" as being the BC formed by 2 c-symmetric channels. Following this same idea, and considering equivalently the Compound BC or the Compound Channel, we can say that the BC resulting from the simultaneity of two c-symmetric BC is c-symmetric.

As it is shown in [29, Lemma 2] that uniform input distribution is optimal for such a channel, we conclude that $X \sim \text{Bern}(1/2)$ is optimal for the Compound BC.

B.6 Proof of Proposition 3

Recall that:

$$t_a(x) \triangleq \sup_{p_{QX}\in\mathcal{C}(x)} \Big[a\, I(Q;Y_1) + \bar{a}\, I(Q;Y_2)\Big] \ . \tag{B.57}$$

We want to show that:

i) For all $x \in [0 : 1 - H_2(p)]$,

$$t_a(x) = \max_{p_{QX}\in\mathcal{C}(x)} \Big[a\, I(Q;Y_1) + \bar{a}\, I(Q;Y_2)\Big] \tag{B.58}$$

ii) t_a is concave in x.

iii) t_a can be described identically by its supporting lines.

iv) t_a is decreasing in x.

Proof: i) We have that:

$$\mathcal{C}(x) = \Big\{ p_{XQ} \in \mathcal{P}(\mathcal{X}\times\mathcal{Q}) : Q \multimap X \multimap (Y, Z_1, Z_2), \tag{B.59}$$
$$X \sim \text{Bern}(1/2),\ I(X;Z|Q) = x \Big\} \ . \tag{B.60}$$

Since, we have proved that the optimizing probabilities have a finite cardinality, the conditional mutual information being continuous, $\mathcal{C}(x)$ is thus compact. As the probability

space $\mathcal{P}(\mathcal{X} \times \mathcal{Q})$ has a finite dimension, the set $\mathcal{C}(x)$ is thus closed. Thus, the supremum is achieved.

ii) Concavity:

Let $x_1, x_2 \in [0 : 1 - H_2(p)]$ and let $\alpha \in [0 : 1]$. Denote $x = \alpha\, x_1 + (1 - \alpha)\, x_2$. We need to show that: $t_a(x) \geq \alpha\, t_a(x_1) + (1 - \alpha)\, t_a(x_2)$.

Let for $i \in \{1, 2\}$,

$$P_{X_i,Q_i} = \underset{p_{QX} \in \mathcal{C}(x)}{\operatorname{argmax}} \Big[a\, I(Q; Y_1) + \bar{a}\, I(Q; Y_2) \Big] \ . \tag{B.61}$$

Define moreover: $T \sim \text{Bern}(t)$ independent of all other RVs. Define

$$(X, Q_T) = \begin{cases} (X_1, Q_1) & \text{if} \quad T = 0 \ , \\ (X_2, Q_2) & \text{if} \quad T = 1 \ , \end{cases} \tag{B.62}$$

and by letting $Q = (Q_T, T)$, we have:

- $X \sim \text{Bern}(1/2)$.
- $Q \multimap X \multimap (Y, Z_1, Z_2)$ is a valid Markov chain.
- And the following equalities hold:

$$\begin{aligned} I(X; Z|Q) &= \alpha\, I(X_1; Z|Q_1) + (1 - \alpha)\, I(X_2; Z|Q_2) && \text{(B.63)} \\ &= \alpha\, x_1 + (1 - \alpha)\, x_2 = x \ . && \text{(B.64)} \end{aligned}$$

We thus have that: $p_{XQ} \in \mathcal{C}(x)$. Thus,

$$\begin{aligned} \alpha\, t_a(x_1) + (1 - \alpha)\, t_a(x_2) &= \alpha \Big(a\, I(Q_1; Y_1) + \bar{a}\, I(Q_1; Y_2) \Big) \\ &\quad + (1 - \alpha) \Big(a\, I(Q_2; Y_1) + \bar{a}\, I(Q_2; Y_2) \Big) && \text{(B.65)} \\ &= a\, I(Q_T; Y_1|T) + (1 - a)\, I(Q_T; Y_2|T) && \text{(B.66)} \\ &\leq a\, I(TQ_T; Y_1) + (1 - a)\, I(TQ_T; Y_2) && \text{(B.67)} \\ &= a\, I(Q; Y_1) + (1 - a)\, I(Q; Y_2) && \text{(B.68)} \\ &\leq \max_{p_{QX} \in \mathcal{C}(x)} \Big[a\, I(Q; Y_1) + (1 - a)\, I(Q; Y_2) \Big] && \text{(B.69)} \\ &= t_a(x) \ , && \text{(B.70)} \end{aligned}$$

which concludes the proof of concavity.

iii) This property follows from the concavity of t_a.

iv) Monotony:

Since t_a is concave, we have that:

$$t'_a(x) \leq t'_a(0) = \lim_{x \to 0^+} \frac{t_a(x) - t_a(0)}{x} \ . \tag{B.71}$$

Since,

$$t_a(0) = a\,(1 - H_2(p_1)) + (1 - a)\,(1 - e_2) > t_a(x) \ , \tag{B.72}$$

for all $x \in [0 : 1 - H_2(p)]$, we have that:

$$t'_a(x) \leq t'_a(0) \leq 0 \ , \tag{B.73}$$

t_a is thus decreasing in x. ■

Appendix C

Proof of results of Chapter 2

C.1 Proof of achievability of Multiple Description inner bound

In this section, we establish the achievability of the MD inner bound (20). Let W_1 be the message decoded by user 1, and let W_2 be the message decoded by user 2, plus let R_1 and R_2 denote their respective rates. Let T_1 and T_2 denote the corresponding binning rates. We construct the following code.

Codebook generation:

Generate $2^{n\,T_1}$ n-sequences $u_0^n(l_1)$, $l_1 \in [1 : 2^{nT_1}]$ each following:

$$P_{U_0}^n(u_0^n(l_1)) = \prod_{i=1}^{n} P_{U_0}(u_{0,i}(l_1)) \ ,$$

and map all these sequences in 2^{nR_1} bins, each indexed with $w_1 \in [1 : 2^{nR_1}]$: $\mathcal{C}_0(w_1)$.

Generate similarly 2^{nT_2} n-sequences $v^n(l_2)$, $l_2 \in [1 : 2^{nT_2}]$ each following $P_V^n(v^n(l_2))$ and map them into 2^{nR_2} bins: $\mathcal{C}_v(w_2)$.

For each $u_0^n(l_1)$, $l_1 \in [1 : 2^{nT_1}]$, generate $2^{n\,\hat{R}_j}$ n-sequences $u_j^n(s_j, l_1)$, $s_j \in [1 : 2^{n\hat{R}_1}]$ following each:

$$P_{U_j|U_0}^n(u_j^n(s_j, l_1)) = \prod_{i=1}^{n} P_{U_j|U_0}(u_{j,i}(s_j, l_j)|u_{0,i}(l_1)) \ .$$

Encoding:

To send a message pair (W_1, W_2), the encoder finds a couple of sequences $u_0^n(l_1)$ and $v^n(l_2)$ in the product bin $\mathcal{C}_0(W_1) \times \mathcal{C}_v(W_2)$ and a couple of indices (s_1, s_2) such that

$$\Big(u_0^n(l_1), u_1^n(s_1, l_1), u_1^n(s_2, l_1), v^n(l_2)\Big) \in T_\delta^n(U_0U_1U_2V) \ . \tag{C.1}$$

It then transmits an n-sequence $x^n\,(u_0^n(l_1), u_1^n(s_1, l_1), u_1^n(s_2, l_1), v^n(l_2))$ which is generated via a random mapping.

Using the well known second order moment method, one can make the probability of

the encoding error event arbitrarily close to 0 if:

$$\begin{cases} T_1 - R_1 + \hat{R}_1 + \hat{R}_2 & \geq & I(U_1; U_2|U_0) \ , \\ T_1 - R_1 + T_2 - R_2 & \geq & I(U_0; V) \ , \\ T_1 - R_1 + \hat{R}_1 + T_2 - R_2 & \geq & I(U_0U_1; V) \ , \\ T_1 - R_1 + \hat{R}_2 + T_2 - R_2 & \geq & I(U_0U_2; V) \ , \\ T_1 - R_1 + \hat{R}_1 + \hat{R}_2 + T_2 - R_2 & \geq & I(U_0U_1U_2; V) + I(U_1; U_2|U_0) \ . \end{cases} \tag{C.2}$$

Proof. A thorough proof is given in Appendix C.2. □

Decoding:

The second user, upon receiving the sequence z^n, looks for the unique index w_2 such that for some $v^n(l_2) \in \mathcal{C}_v(w_2)$, the following holds:

$$\left(v^n(l_2), z^n\right) \in T_\delta^n(VZ) \ . \tag{C.3}$$

The probability of error in such a decoding rule is arbitrarily small provided that:

$$T_2 \leq I(V; Z) \ . \tag{C.4}$$

Concerning the two instances of the first user Y_1 and Y_2 let us assimilate each of them to a decoder. Decoder j finds the unique index l_1 such that for some s_j where, the following joint typicality holds:

$$\left(u_0^n(l_1), u_j^n(s_j, l_1), y_j^n\right) \in T_\delta^n(U_0U_jY_j) \ . \tag{C.5}$$

The probability that the decoded l_1 does not fall into the bin specified by w_1 is made arbitrarily provided that:

$$T_1 + \hat{R}_j \leq I(U_0U_j; Y_j) \ . \tag{C.6}$$

Then the overall decoding error events occur with arbitrary small probability provided that:

$$\begin{cases} T_1 + \hat{R}_1 & \leq & I(U_0U_1; Y_j) \ , \\ T_1 + \hat{R}_2 & \leq & I(U_0U_2; Y_j) \ , \\ T_2 & \leq & I(V; Z) \ . \end{cases} \tag{C.7}$$

After running FME on the system of inequalities bearing in mind the natural encoding constraints:

$$\begin{cases} \hat{R}_1 & \geq & 0 \ , \\ \hat{R}_2 & \geq & 0 \ , \\ T_1 & \geq & R_1 \ , \\ T_2 & \geq & R_2 \ , \end{cases} \tag{C.8}$$

the region given in (20) follows immediately.

C.2 Proof of the covering lemma in Appendix C.1

In this section, we give a thorough proof of the multivariate covering lemma used in multiple description coding C.1.

To this end, let us recall the claim we are showing. Let $u^n(l_1)$ be the 2^{nT_1} codewords carrying the common description of user 1 and mapped in 2^{nR_1} bins $\mathcal{B}_1^n(w_1)$. Let $v^n(l_2)$ be the 2^{nT_2} private codewords of user 2 mapped in 2^{nR_2} bins $\mathcal{B}_2^n(w_2)$. $v^n(l_2)$ and $u^n(l_1)$ are generated independently. Let $u_1^n(s_1, l_1)$ and $u_2^n(s_2, l_1)$ be two private descriptions generated independently and conditionally on $u^n(l_1)$ with respective rates $2^{n\hat{R}_1}$ and $2^{n\hat{R}_2}$. Let us denote the rates inside the respective bins by $L_1 = T_1 - R_1$ and $L_2 = T_2 - R_2$

Define the list $\mathcal{A}(w_1, w_2)$ as the set of quadruples of indices (l_1, s_1, s_2, l_2) that satisfy:

$$\mathcal{A}(w_1, w_2) = \Bigg\{ \begin{array}{l} (l_1, s_1, s_2, l_2) \text{ s.t, } \ (s_1, s_2) \in [1 : 2^{n\hat{R}_1}] \times [1 : 2^{n\hat{R}_2}] \ , \\ (u^n(l_1), v^n(l_2)) \in \mathcal{B}_1^n(w_1) \times \mathcal{B}_2^n(w_2) \ , \\ (u^n(l_1), u_1^n(s_1, l_1), u_2^n(s_2, l_1), v^n(l_2)) \in T_\delta^n(UU_1U_2V) \end{array} \Bigg\} . \tag{C.9}$$

The encoding is successful if,

$$\forall (w_1, w_2) \in \mathcal{M}_1 \times \mathcal{M}_2 \quad , \quad \|\mathcal{A}(w_1, w_2)\| \neq 0 \ . \tag{C.10}$$

It can easily be shown that:

$$P(\text{Encoding error}) = \mathbb{P}\Big(\exists (W_1, W_2) \ , \ \|\mathcal{A}(W_1, W_2)\| = 0\Big) \leq \mathbb{P}\Big(\|\mathcal{A}(1,1)\| = 0\Big) \ . \tag{C.11}$$

We define then more specifically:

$$\mathcal{A} \triangleq \mathcal{A}(1,1) \tag{C.12}$$
$$E(l_1, s_1, s_2, l_2) \triangleq \mathbb{1}\Big\{(l_1, s_1, s_2, l_2) \in \mathcal{A}\Big\} \tag{C.13}$$
$$P(l_1, s_1, s_2, l_2) \triangleq \mathbb{P}(E(l_1, s_1, s_2, l_2) = 1) \tag{C.14}$$
$$P(l_1, s_1, s_2, l_2, l_1', s_1', s_2', l_2') \triangleq \mathbb{P}(E(l_1, s_1, s_2, l_2) = 1, E(l_1', s_1', s_2', l_2') = 1) \tag{C.15}$$

The probability of encoding error can then be bounded as:

$$P(\text{Encoding error}) \leq \mathbb{P}\Big(\|\mathcal{A}\| = 0\Big) \leq \frac{Var(\|\mathcal{A}\|)}{\mathbb{E}^2(\|\mathcal{A}\|)} \ . \tag{C.16}$$

Thus, in the sequel we bound both $Var(\|\mathcal{A}\|)$ and $\mathbb{E}^2(\|\mathcal{A}\|)$.

Note that in the following, when a quadruple of indices (l_1, s_1, s_2, l_2), is considered, then it is implicit that $(u^n(l_1), v^n(l_2)) \in \mathcal{B}_1^n(1) \times \mathcal{B}_2^n(1)$ and that $(s_1, s_2) \in [1 : 2^{n\hat{R}_1}] \times [1 : 2^{n\hat{R}_2}]$, thus belonging to the set $\mathcal{A}$ relies only on the typicality condition:

$$(u^n(l_1), u_1^n(s_1, l_1), u_2^n(s_2, l_1), v^n(l_2)) \in T_\delta^n(UU_1U_2V) \tag{C.17}$$

We will also note in the following: $\exp_2^n(x) \triangleq 2^{nx}$

C.2.1 Bounding $\mathbb{E}^2(\|\mathcal{A}\|)$

We start by writing with standard manipulations that:

$$\mathbb{E}(\|\mathcal{A}\|) = \sum_{l_1,s_1,s_2,l_2} P(l_1,s_1,s_2,l_2) \tag{C.18}$$

$$\geq \exp_2^n\Big(L_1 + \hat{R}_1 + \hat{R}_2 + L_2 - I(UU_1U_2;V) - I(U_1;U_2|U) - \epsilon_n]\Big) \tag{C.19}$$

Thus,

$$\mathbb{E}^2(\|\mathcal{A}\|) \geq \exp_2^n\Big(2[L_1 + \hat{R}_1 + \hat{R}_2 + L_2 - I(UU_1U_2;V) - I(U_1;U_2|U) - \epsilon_n]\Big) \tag{C.20}$$

C.2.2 Bounding $Var(\|\mathcal{A}\|)$

To bound the variance, we start by writing that:

$$Var(\|\mathcal{A}\|) = \mathbb{E}(\|\mathcal{A}\|^2) - \mathbb{E}^2(\|\mathcal{A}\|) \tag{C.21}$$

all is left then is to bound the term: $\mathbb{E}(\|\mathcal{A}\|^2)$.

We have that:

$$\mathbb{E}(\|\mathcal{A}\|^2) = \sum_{l_1,s_1,s_2,l_2} \sum_{l_1',s_1',s_2',l_2'} P(l_1,s_1,s_2,l_2,l_1',s_1',s_2',l_2') \tag{C.22}$$

Moreover,

$$\sum_{l_1,s_1,s_2,l_2} \sum_{l_1',s_1',s_2',l_2'} P(l_1,s_1,s_2,l_2,l_1',s_1',s_2',l_2') \tag{C.23}$$

$$= \sum_{l_1,s_1,s_2,l_2} P(l_1,s_1,s_2,l_2) + \sum_{l_1,s_1,s_2,l_2} \sum_{l_1'\neq l_1} P(l_1,s_1,s_2,l_2,l_1',s_1,s_2,l_2)$$

$$+ \sum_{l_1,s_1,s_2,l_2} \sum_{l_2'\neq l_2} P(l_1,s_1,s_2,l_2,l_1,s_1,s_2,l_2') + \sum_{l_1,s_1,s_2,l_2} \sum_{s_1'\neq s_1} P(l_1,s_1,s_2,l_2,l_1,s_1',s_2,l_2)$$

$$+ \sum_{l_1,s_1,s_2,l_2} \sum_{s_2'\neq s_2} P(l_1,s_1,s_2,l_2,l_1,s_1,s_2',l_2) + \sum_{l_1,s_1,s_2,l_2} \sum_{\substack{s_1'\neq s_1\\ s_2'\neq s_2}} P(l_1,s_1,s_2,l_2,l_1,s_1',s_2',l_2)$$

$$+ \sum_{l_1,s_1,s_2,l_2} \sum_{\substack{l_1'\neq l_1\\ s_1'\neq s_1}} P(l_1,s_1,s_2,l_2,l_1',s_1',s_2,l_2) + \sum_{l_1,s_1,s_2,l_2} \sum_{\substack{l_1'\neq l_1\\ s_2'\neq s_2}} P(l_1,s_1,s_2,l_2,l_1',s_1,s_2',l_2)$$

$$+ \sum_{l_1,s_1,s_2,l_2} \sum_{\substack{s_1'\neq s_1\\ l_2'\neq l_2}} P(l_1,s_1,s_2,l_2,l_1,s_1',s_2,l_2') + \sum_{l_1,s_1,s_2,l_2} \sum_{\substack{s_2'\neq s_2\\ l_2'\neq l_2}} P(l_1,s_1,s_2,l_2,l_1,s_1,s_2',l_2')$$

$$+ \sum_{l_1,s_1,s_2,l_2} \sum_{\substack{l_1'\neq l_1\\ l_2'\neq l_2}} P(l_1,s_1,s_2,l_2,l_1',s_1,s_2,l_2') + \sum_{l_1,s_1,s_2,l_2} \sum_{\substack{l_1'\neq l_1\\ s_1'\neq s_1\\ s_2'\neq s_2}} P(l_1,s_1,s_2,l_2,l_1',s_1',s_2',l_2)$$

$$+ \sum_{l_1,s_1,s_2,l_2} \sum_{\substack{l_1'\neq l_1\\ s_1'\neq s_1\\ l_2'\neq l_2}} P(l_1,s_1,s_2,l_2,l_1',s_1',s_2,l_2') + \sum_{l_1,s_1,s_2,l_2} \sum_{\substack{l_1'\neq l_1\\ s_2'\neq s_2\\ l_2'\neq l_2}} P(l_1,s_1,s_2,l_2,l_1',s_1,s_2',l_2')$$

$$+\sum_{l_1,s_1,s_2,l_2}\sum_{\substack{s_1'\neq s_1\\ s_2'\neq s_2\\ l_2'\neq l_2}} P(l_1,s_1,s_2,l_2,l_1,s_1',s_2',l_2') + \sum_{l_1,s_1,s_2,l_2}\sum_{\substack{l_1'\neq l_1\\ s_1'\neq s_1\\ s_2'\neq s_2\\ l_2'\neq l_2}} P(l_1,s_1,s_2,l_2,l_1',s_1',s_2',l_2') \tag{C.24}$$

Since all operands are symmetric in s_1 and s_2, we will bound only representative terms.

- Bounding $P(l_1,s_1,s_2,l_2,l_1',s_1,s_2,l_2)$.

$$\begin{aligned}
&P(l_1,s_1,s_2,l_2,l_1',s_1,s_2,l_2)\\
&=\sum_{v^n\in T_\delta^n(V)} P(V^n=v^n)\Big[\mathbb{P}\Big((U^n(l_1),U_1^n(s_1,l_1),U_2^n(s_2,l_1))\in T_\delta^n(UU_1U_2|v^n)\Big)\Big]^2\\
&\leq\sum_{v^n\in T_\delta^n(V)} P(V^n=v^n)\Big[\exp_2^n\Big(H(UU_1U_2|V)-H(U)-H(U_1|U)-H(U_2|U)+\epsilon_n\Big)\Big]^2\\
&=\exp_2^n\Big(-2[I(UU_1U_2;V)+I(U_1;U_2|U)-\epsilon_n]\Big)\sum_{v^n\in T_\delta^n(V)} P(V^n=v^n) &\text{(C.25)}\\
&\leq\exp_2^n\Big(-2[I(UU_1U_2;V)+I(U_1;U_2|U)-\epsilon_n]\Big) &\text{(C.26)}
\end{aligned}$$

- Bounding $P(l_1,s_1,s_2,l_2,l_1,s_1,s_2,l_2')$. Similarly, we can write:

$$\begin{aligned}
&P(l_1,s_1,s_2,l_2,l_1,s_1,s_2,l_2')\\
&=\sum_{\substack{(u^n,u_1^n,u_2^n)\\ \in T_\delta^n(UU_1U_2)}} P\Big((U^n(l_1),U_1^n(s_1,l_1),U_2^n(s_2,l_1)=(u^n,u_1^n,u_2^n)\Big)\Big[\mathbb{P}\Big(V^n(l_2)\in T_\delta^n(V|u^nu_1^nu_2^n)\Big)\Big]^2\\
&\leq\exp_2^n\Big(-[I(U_1;U_2|U)-\epsilon_n]\Big)\exp_2^n\Big(-2[I(UU_1U_2;V)-\epsilon_n]\Big) &\text{(C.27)}\\
&=\exp_2^n\Big(-[I(U_1;U_2|U)+2I(UU_1U_2;V)-3\epsilon_n]\Big) &\text{(C.28)}
\end{aligned}$$

- Bounding $P(l_1,s_1,s_2,l_2,l_1,s_1',s_2,l_2)$. To this end, we write:

$$\begin{aligned}
&P(l_1,s_1,s_2,l_2,l_1,s_1',s_2,l_2)\\
&=\sum_{\substack{(u^n,u_2^n,v^n)\\ \in T_\delta^n(UU_2V)}} P\Big((U^n(l_1),U_2^n(s_2,l_1),V^n(l_2))=(u^n,u_2^n,v^n)\Big)\Big[\mathbb{P}\Big(U_1^n(s_1,l_1)\in T_\delta^n(U_1|u^nu_2^nv^n)\Big)\Big]^2\\
&\leq\exp_2^n\Big(-[I(UU_2;V)-\epsilon_n]\Big)\exp_2^n\Big(-2[I(U_1;VU_2|U)-\epsilon_n]\Big) &\text{(C.29)}\\
&=\exp_2^n\Big(-[I(UU_2;V)+2I(U_1;VU_2|U)-3\epsilon_n]\Big) &\text{(C.30)}
\end{aligned}$$

- Bounding $P(l_1,s_1,s_2,l_2,l_1,s_1',s_2',l_2)$. We write:

$$P(l_1,s_1,s_2,l_2,l_1,s_1',s_2',l_2)$$

$$= \sum_{\substack{(u^n,v^n)\\ \in T_\delta^n(UV)}} P\Big((U^n(l_1), V^n(l_2)) = (u^n, v^n)\Big)\Big[\mathbb{P}\Big((U_1^n(s_1,l_1), U_2^n(s_2,l_1)) \in T_\delta^n(U_1U_2|u^nv^n)\Big)\Big]^2$$

$$\leq \exp_2^n\Big(-[I(U;V) - \epsilon_n]\Big)\exp_2^n\Big(-2[I(U_1U_2;V|U) + I(U_1;U_2|U) - \epsilon_n]\Big) \tag{C.31}$$

$$= \exp_2^n\Big(-[I(U;V) + 2I(U_1;U_2|U) + 2I(U_1U_2;V|U) - 3\epsilon_n]\Big) \tag{C.32}$$

- Bounding $P(l_1, s_1, s_2, l_2, l_1', s_1', s_2, l_2)$. We have that:

$$P(l_1, s_1, s_2, l_2, l_1', s_1', s_2, l_2)$$

$$\leq \Big[\mathbb{P}\Big((u^n(l_1), u_1^n(s_1,l_1), u_2^n(s_2,l_1), v^n(l_2)) \in T_\delta^n(UU_1U_2V)\Big)\Big]^2 \tag{C.33}$$

$$\leq \exp_2^n\Big(-2[I(UU_1U_2;V) + I(U_1;U_2|U) - \epsilon_n]\Big) \tag{C.34}$$

- The remaining terms given by: $P(l_1, s_1, s_2, l_2, l_1', s_1, s_2, l_2')$, $P(l_1, s_1, s_2, l_2, l_1, s_1', s_2, l_2')$, $P(l_1, s_1, s_2, l_2, l_1', s_1', s_2, l_2')$, $P(l_1, s_1, s_2, l_2, l_1', s_1', s_2', l_2)$, $P(l_1, s_1, s_2, l_2, l_1, s_1', s_2', l_2')$, and $P(l_1, s_1, s_2, l_2, l_1', s_1', s_2', l_2')$, can all be upper bounded by:

$$\exp_2^n\Big(-2[I(UU_1U_2;V) + I(U_1;U_2|U) - \epsilon_n]\Big) \tag{C.35}$$

C.2.3 Bounding the probability of encoding error

Going back the equation (C.24), we carry on writing each term in the summation as follows:

$$\frac{Var(\|\mathcal{A}\|)}{\mathbb{E}^2(\|\mathcal{A}\|)}$$

$$\leq \exp_2^n\Big(-L_1 - \hat{R}_1 - \hat{R}_2 - L_2 + I(UU_1U_2;V) + I(U_1;U_2|U) + \epsilon_n]\Big)$$
$$+ \exp_2^n\Big(-\hat{R}_1 - \hat{R}_2 - L_2 + \epsilon_n\Big) + \exp_2^n\Big(-\hat{R}_1 - \hat{R}_2 - L_1 + \epsilon_n\Big)$$
$$+ \exp_2^n\Big(-L_1 - \hat{R}_2 - L_2 + I(UU_2;V) + \epsilon_n\Big) + \exp_2^n\Big(-L_1 - \hat{R}_1 - L_2 + I(UU_1;V) + \epsilon_n\Big)$$
$$+ \exp_2^n\Big(-L_1 - L_2 + I(U;V) + \epsilon_n\Big) + \exp_2^n\Big(-\hat{R}_2 - L_2 + \epsilon_n\Big) + \exp_2^n\Big(-\hat{R}_1 - L_2 + \epsilon_n\Big)$$
$$+ \exp_2^n\Big(-L_1 - \hat{R}_2 + \epsilon_n\Big) + \exp_2^n\Big(-L_1 - \hat{R}_1 + \epsilon_n\Big) + \exp_2^n\Big(-\hat{R}_1 - \hat{R}_2 + \epsilon_n\Big)$$
$$+ \exp_2^n\Big(-L_2 + \epsilon_n\Big) + \exp_2^n\Big(-L_1 + \epsilon_n\Big) + \exp_2^n\Big(-\hat{R}_2 + \epsilon_n\Big) + \exp_2^n\Big(-\hat{R}_1 + \epsilon_n\Big) \tag{C.36}$$

Thus, to have the probability of encoding error arbitrarily small, one only needs to ensure that:

$$L_1 + \hat{R}_1 + \hat{R}_2 + L_2 \geq I(UU_1U_2;V) + I(U_1;U_2|U) \tag{C.37}$$

$$L_1 + \hat{R}_2 + L_2 \geq I(UU_2;V) \tag{C.38}$$

$$L_1 + \hat{R}_1 + L_2 \geq I(UU_1; V) \tag{C.39}$$
$$L_1 + L_2 \geq I(U; V) \tag{C.40}$$

Which comes in fine to:

$$T_1 - R_1 + \hat{R}_1 + \hat{R}_2 + T_2 - R_2 \geq I(UU_1U_2; V) + I(U_1; U_2|U) \tag{C.41}$$
$$T_1 - R_1 + \hat{R}_2 + T_2 - R_2 \geq I(UU_2; V) \tag{C.42}$$
$$T_1 - R_1 + \hat{R}_1 + T_2 - R_2 \geq I(UU_1; V) \tag{C.43}$$
$$T_1 - R_1 + T_2 - R_2 \geq I(U; V) \tag{C.44}$$

C.3 Proof of Lemma 1

We derive the optimal rate obtained when the following coding scheme is used:

$$\mathbf{X} = (X_u + X_p)\mathbf{B}_u + X_v\mathbf{B}_v \ , \qquad U_0 = X_u + \alpha X_v \ , \tag{C.45}$$
$$V = X_v \ , \qquad U_1 = X_p + \alpha_1 X_v \ , \tag{C.46}$$

where $X_p \sim \mathcal{N}(0, x)$, $X_u \sim \mathcal{N}(0, P_u - x)$ and $X_v \sim \mathcal{N}(0, P_v)$ are pairwise independent RV and such that: $P_u \leq P - P_v$.
This means that we transmit two descriptions intended for user 1 making these two descriptions compensate "jointly" the interference, hence, we are interested in computing the rate: $R_{0,1} = I(U_0U_1; Y) - I(U_0U_1; V)$. Some algebraic manipulations lead us to the following result:

$$R_{0,1} = \frac{1}{2}\log_2\left(\frac{h_u^2 P_u + N}{\frac{P_v\,(h_u^2 P_u + N)}{h_u^2 P_u + h_v^2 P_v + N}P(\alpha, \alpha_1) + N}\right) \ , \tag{C.47}$$

where the quadratic polynomial $P(\alpha, \alpha_1)$ is given by:

$$P(\alpha, \alpha_1) = h_u^2(\alpha_1 - \beta_1^x + \alpha - \beta^x)^2 + \frac{N}{x}(\alpha_1 - \beta_1^x)^2 + \frac{N}{P_u - x}(\alpha - \beta^x)^2 \ , \tag{C.48}$$

and, $\beta^x = \dfrac{(P_u - x)\,h_u\,h_v}{h_u^2 P_u + N}$ and $\beta_1^x = \dfrac{x\,h_u\,h_v}{h_u^2 P_u + N}$.

An interesting insight brought by this expression is that to achieve the optimal DoF, we need only have $\alpha_1 + \alpha = \beta_1^o + \alpha^o$ rather than pairwise equality as might be suggested by the previous section. This translates perfectly the "joint" interference management of both decoded descriptions U_0 and U_1, recovering trivially the optimal interference free rate as both descriptions cancel the interference fully each on their own $\alpha_1 - \alpha_1^\star = \alpha_0 - \alpha_0^\star = 0$.

Upon optimizing the polynomial $P(\alpha, \alpha_1)$ over α_1, the resulting rate is given by the rather simple expression:

$$R_{0,1} = \frac{1}{2}\log_2\left(\frac{h_u^2 P_u + N}{\frac{P_v}{(P_u - x)}\frac{(h_u^2\ P_u + N)^2}{(h_u^2 P_u + h_v^2 P_v + N)}\frac{N}{h_u^2 x + N}(\alpha - \beta^x)^2 + N}\right) \ , \tag{C.49}$$

It can be readily checked that this expression corresponds to the following formulation of the rate:

$$R_{0,1} = I(U_0;Y) - I(U_0;V) + I(X_p;Y|X_uX_v) \ , \tag{C.50}$$

where

$$I(X_p;Y|X_uX_v) = \frac{1}{2}\log_2\left(\frac{h_u^2x+N}{N}\right) \ , \tag{C.51}$$

and where $I(U_0;Y) - I(U_0;V)$ corresponds to the case where X_u dirty-paper codes X_v under the noise component variance: $h_u^2x + N$.

This means that the optimal choice of the variable U_1 is the one that maximizes the DPC term $I(U_1;Y|U_0) - I(U_1;V|U_0)$.

C.4 Optimization of Common Description inner bound:

Let us first optimize the second corner point of the CD inner bound. We have that

$$\begin{aligned}\mathcal{R}_2 = \Bigg\{(R_1,R_2)\in\mathbb{R}_+^2 \ , \quad R_2 &\leq \frac{1}{2}\log_2\left(\frac{g_v^2P_v+N}{N}\right) \ , \\ R_1 &\leq \min_{j=1,2}\frac{1}{2}\log_2\left(\frac{h_{j,u}^2P_u+h_{j,v}^2P_v+N}{h_{j,v}^2P_v+N}\right)\Bigg\} \ .\end{aligned} \tag{C.52}$$

We have that what maximizes $\mathbf{h}_1$ and $\mathbf{h}_2$ are orthogonal and of unit norm, thus, we can write that: $h_{1,u}^2 = 1 - h_{2,u}^2$ and $h_{1,v}^2 = 1 - h_{2,v}^2$. The rate R_2 does not depend on the beam $\mathbf{B}_u$, thus, we start by optimizing the rate R_1 over it. The two min operands are monotonic in inverse directions and have the same minimum value 0, thus, the maxmin point corresponds to the equality point. Which by simple algebraic calculations leads to the condition:

$$h_{1,u}^2 = \frac{h_{1,v}^2P_v+N}{P_v+2N} \ , \tag{C.53}$$

and yields then a rate (independent of the beam $\mathbf{B}_v$) equal to:

$$R_1 \leq \frac{1}{2}\log_2\left(\frac{P_u+P_v+2N}{P_v+2N}\right) \ . \tag{C.54}$$

Note then that the maximizing beam direction $\mathbf{B}_v = \mathbf{g}$, thus one can easily check that this verifies: $h_{1,v} = -1/\sqrt{2}$ and thus, from (C.54), that $|h_{1,u}| = 1/\sqrt{2}$. Thus transmitting the first user's signal in the mean channel direction is an admissible optimizing solution. Later in the proof, we show that this corner point is dominated by the first corner point of the CD inner bound. In the sequel, we will perform the optimization under the choice of $h_{1,u} = 1/\sqrt{2}$ and $g_u = 0$, i.e., we transmit the signal intended to user 1 in the mean channel direction, which makes it orthogonal to the second user's channel; the optimality of which is given in Appendix C.5.

We can rewrite the first corner point of the CD inner bound as follows:

$$\mathcal{R}_1 = \bigcup_{a\in[0:1]} \Bigg\{ (R_1,R_2) \in \Re_+^2, \quad R_1 \leq \max_{\alpha\in\mathbb{R}} \min_{j\in\{1,2\}} \frac{1}{2}\log_2\left(\frac{P_u+2N}{\frac{P_v}{P_u}\frac{(P_u+2N)^2}{P_u+2N+2h_{j,v}^2P_v}(\alpha-\alpha_j)^2+2N}\right) \quad R_2 \leq \frac{1}{2}\log_2\left(\frac{g_v^2P_v+N}{N}\right)\Bigg\} \tag{C.55}$$

where $\alpha_j = \dfrac{\sqrt{2}P_u}{P_u+2N}h_{j,v}$. Since $\|\mathbf{h}_j\| = \|\mathbf{B}_v\| = 1$ and, $\mathbf{h}_1$ and $\mathbf{h}_2$ are orthogonal, we can let $h_{1,v} = \cos(\theta_v)$ and $h_{2,v} = \sin(\theta_v)$.

The key point in the optimization is to solve the equation:

$$\frac{(\alpha-\alpha_1)^2}{P_u+2N+2\cos(\theta_v)^2P_v} = \frac{(\alpha-\alpha_2)^2}{P_u+2N+2\sin(\theta_v)^2P_v}\ . \tag{C.56}$$

The optimization of the rate of the first user R_1 yields the following:

(i) If $\cos^2(\theta_v) = \dfrac{1}{2}$ and $\cos(\theta_v) = -\sin(\theta_v)$, then the optimal rate is given by:

$$R_1 \leq \max_{\alpha} \min_{j\in\{1,2\}} \frac{1}{2}\log_2\left(\frac{P_u+2N}{\frac{P_v}{P_u}\frac{(P_u+2N)^2}{(P+2N)}(\alpha-\alpha_j)^2+2N}\right) \tag{C.57}$$

$$= \max_{\alpha} \frac{1}{2}\log_2\left(\frac{P_u+2N}{\frac{P_v}{P_u}\frac{(P_u+2N)^2}{(P+2N)}(|\alpha|+|\alpha_j|)^2+2N}\right) \tag{C.58}$$

$$= \frac{1}{2}\log_2\left(\frac{P_u+2N}{2N+P_v\frac{P_u}{P+2N}}\right) \tag{C.59}$$

$$= \frac{1}{2}\log_2\left(\frac{P_u+P_v+2N}{P_v+2N}\right) \tag{C.60}$$

where $\alpha_1 = -\alpha_2 = \dfrac{P_u}{P_u+2N}$. It turns out then, that the optimization over the DPC parameter α yields $\alpha = 0$, i.e. the dilemma at the transmitter is so strong that the optimal choice is not to cancel interference and send in a direction that does not yield privilege to any of the channel instances $\mathbf{h}$. A very important remark, is that this yields exactly the first corner point of the region.

(ii) If $\cos^2(\theta_v) = \frac{1}{2}$ and $\cos(\theta_v) = \sin(\theta_v)$, then the optimal rate is given by:

$$R_1 \leq \frac{1}{2}\max_{\alpha} \min_{j\in\{1,2\}} \log_2 \left(\frac{P_u + 2N}{\frac{P_v}{P_u}\frac{(P_u+2N)^2}{(P+2N)}(\alpha-\alpha_j)^2 + 2N} \right) \tag{C.61}$$

$$= \frac{1}{2}\log_2\left(\frac{P_u+2N}{2N}\right) , \tag{C.62}$$

which corresponds to the point where $h_{1,v} = h_{2,v}$ i.e. $\alpha_1 = \alpha_2$. Thus, we would have $\mathbf{h}_1 - \mathbf{h}_2$ orthogonal to $\mathbf{B}_v$, but since $\mathbf{h}_1 - \mathbf{h}_2$ is collinear to the second user's channel, then it means that no information is transmitted to it with the beam $\mathbf{B}_v$. The power optimization of this point corresponds to the corner point $(C_1, 0)$.

(iii) If $\cos^2(\theta_v) \neq \frac{1}{2}$, then there are two optimizing solutions $\alpha_1^\star$ and $\alpha_2^\star$ such that:

$$\alpha_1^\star - \alpha_1 = \frac{P_u}{P_u+2N} \frac{(-\cos(\theta_v)+\sin(\theta_v))\sqrt{P_u/2+N+\cos(\theta_v)^2P_v}}{\sqrt{P_u+2N+2\sin^2(\theta_v)P_v}+\sqrt{P_u+2N+2\cos^2(\theta_v)P_v}} , \tag{C.63}$$

$$\alpha_2^\star - \alpha_1 = \frac{P_u}{P_u+2N} \frac{(\cos(\theta_v)-\sin(\theta_v))\sqrt{P_u/2+N+\cos(\theta_v)^2P_v}}{\sqrt{P_u+2N+2\sin^2(\theta_v)P_v}-\sqrt{P_u+2N+2\cos^2(\theta_v)P_v}} . \tag{C.64}$$

The root that yields the greater rate is $\alpha_1^\star$. Then, we can rewrite with the following transformation $y = \sin(2\theta_v)$ that:

$$(\alpha_1^\star - \alpha_1)^2$$

$$= \frac{2P_u^2}{(P_u+2N)^2} \frac{\cos^2(\theta_v+\pi/4) \quad (P_u/2+N+\cos(\theta_v)^2P_v)}{\left(\sqrt{P_u+2N+2\sin^2(\theta_v)P_v}+\sqrt{P_u+2N+2\cos^2(\theta_v)P_v}\right)^2} \tag{C.65}$$

$$= \frac{P_u^2}{2(P_u+2N)^2} \frac{(1-y) \quad (P_u/2+N+\cos(\theta_v)^2P_v)}{P+2N+\sqrt{(P_u+2N)(P+2N+P_v)+y^2P_v^2}} \tag{C.66}$$

$$= \frac{P_u^2}{2(P_u+2N)^2} \frac{(1-y) \quad (P_u/2+N+\cos(\theta_v)^2P_v)}{P+2N+\sqrt{(P+2N)^2+(y^2-1)P_v^2}} . \tag{C.67}$$

Note that the value of $y = -1$, i.e., $\theta_v = -\pi/4$, is included in this expression. Thus we drop the case distinctions $\cos^2(\theta_v) = 1/2$ and $\cos^2(\theta_v) \neq 1/2$.

As a conclusion, CD inner bound writes as:

$$\mathcal{R}_{CD} = \bigcup_{y\in[-1:1]} \Bigg\{ (R_1, R_2) \in \Re_+^2 , \\ R_1 \leq \frac{1}{2}\log_2\left(\frac{P_u + 2N}{\frac{P_v P_u(1-y)}{P+2N+\sqrt{(P+2N)^2+(y^2-1)P_v^2}} + 2N}\right) \\ R_2 \leq \frac{1}{2}\log_2\left(\frac{(1-y)P_v + 2N}{2N}\right) \Bigg\} . \tag{C.68}$$

C.5 Beamforming optimization for the CD-DPC inner bound

In this section, we show, that with a strong uncertainty over the channel instances of user 1, i.e., $\mathbf{h}_1$ and $\mathbf{h}_2$ being orthogonal, when resorting to a CD-DPC, the source has no choice but to send over the mean channel $\mathbf{h}_{1,2}$. The proof of this claim is quite evolved and requires the use of many analytical manipulations when solving optimization problems.

Let us use the following notations. We previously introduced θ_v such that $h_{1,v} = \cos(\theta_v)$ and $h_{2,v} = \sin(\theta_v)$. Since $\|\mathbf{h}_j\| = \|\mathbf{B}_u\| = 1$ and, $\mathbf{h}_1$ and $\mathbf{h}_2$ are orthogonal, we can similarly define θ_u such that $h_{1,u} = \cos(\theta_u)$ and $h_{2,u} = \sin(\theta_u)$. Let us define:

$$s_u \triangleq \frac{\sin(2\theta_u)}{|\sin(2\theta_u)|} \text{ and } s_v \triangleq \frac{\sin(2\theta_v)}{|\sin(2\theta_v)|} , \tag{C.69}$$

when $\sin(2\theta_u) \neq 0$ and $\sin(2\theta_v) \neq 0$.

In this section, we prove that it is optimal to transmit the signal in the directions given by: $\mathcal{B}_u = \mathbf{h}_{1,2}$, which comes to having $h_{1,u} = h_{1,v} = \frac{1}{\sqrt{2}}$.

Thus, we need to solve the optimization problem given by:

$$\bigcup_{\mathcal{B}_u,\mathcal{B}_v} \begin{cases} R_1 \leq \max\limits_{\alpha} \min\limits_{j=1,2} \log_2\left(\frac{1}{A_j(\alpha-\alpha_j)^2 + c_j}\right) , \\ R_2 \leq \log_2\left(1 + \frac{g_v^2}{g_u^2 P_u + N}\right) , \end{cases} \tag{C.70}$$

where:

$$A_j \triangleq \frac{P_v}{P_u}\frac{h_{j,u}^2 P_u + N}{h_{j,u}^2 P_u + h_{j,v}^2 P_v + N} , \tag{C.71}$$

$$c_j \triangleq \frac{N}{h_{j,u}^2 P_u + N} , \tag{C.72}$$

$$\text{and} \qquad \alpha_j \triangleq P_u \frac{h_{j,u} h_{j,v}}{h_{j,u}^2 P_u + N} \ . \tag{C.73}$$

This, in part, requires solving the following optimization problem:

$$\max_{\alpha} \min_{j=1,2} \log_2 \left(\frac{1}{A_j \alpha^2 - 2B_j \alpha + D_j} \right) \ , \tag{C.74}$$

where:

$$B_j \triangleq P_v \frac{h_{j,u} h_{j,v}}{h_{j,u}^2 P_u + h_{j,v}^2 P_v + N} \ , \tag{C.75}$$

$$\text{and} \qquad D_j \triangleq \frac{h_{j,v}^2 P_v + N}{h_{j,u}^2 P_u + h_{j,v}^2 P_v + N} \ . \tag{C.76}$$

Finding the optimal DPC parameter α to use requires solving the equation:

$$(A_1 - A_2)\alpha^2 - 2(B_1 - B_2)\alpha + (D_1 - D_2) = 0 \ , \tag{C.77}$$

which yields:

- a) If $A_1 = A_2$ and $B_1 = B_2$ while $D_1 \neq D_2$, no solution exists,
- b) If $A_1 = A_2$ and $B_1 = B_2$ and $D_1 = D_2$, every α is a solution,
- c) If $A_1 = A_2$ and $B_1 \neq B_2$, then there exists only one solution: $\alpha_{opt} = \dfrac{D_1 - D_2}{2(B_1 - B_2)}$,
- d) If $A_1 \neq A_2$ and $(B_1 - B_2)^2 = (A_1 - A_2)(D_1 - D_2)$, then there exists only one solution: $\alpha_{opt} = \dfrac{B_1 - B_2}{A_1 - A_2}$,
- e) If $A_1 \neq A_2$ and $(B_1 - B_2)^2 < (A_1 - A_2)(D_1 - D_2)$ no solution exists,
- f) $A_1 \neq A_2$ and $(B_1 - B_2)^2 > (A_1 - A_2)(D_1 - D_2)$ then there exist two solutions.

Next, we can deduce the optimal values of (C.74) to be used by the source as given in table C.1. Our aim is to show that, over all these cases, the optimal beamforming strategy is to let $\mathbf{B}_u = \mathbf{h}_{1,2}$.

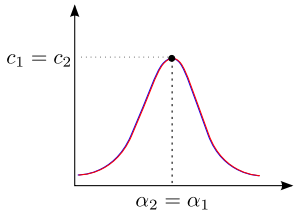
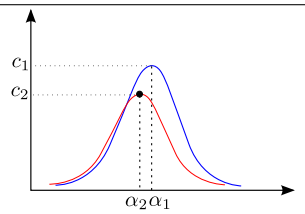
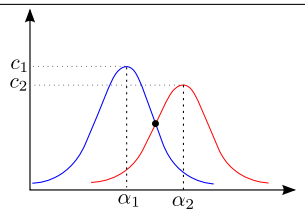
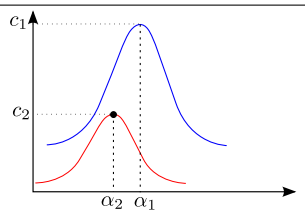
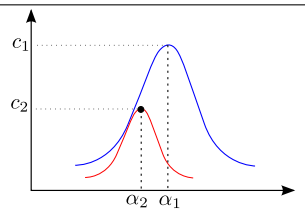
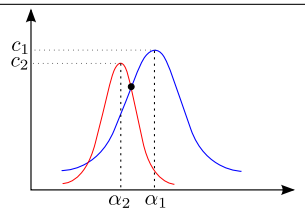
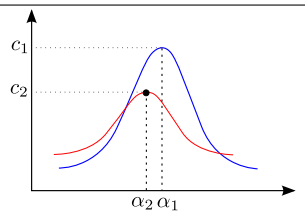
C.5.1 Case of $A_1 = A_2$ and $B_1 = B_2$

We show in the following that if $A_1 = A_2$ and $B_1 = B_2$, then it follows that $D_1 = D_2$ and that $h_{j,u} = -h_{j,v} = \dfrac{1}{\sqrt{2}}$. Thus letting $\mathbf{B}_u = \mathbf{h}_{1,2}$ would yield the optimal solution given by:

$$\min_{\alpha} \max_{j=1,2} A_j(\alpha - \alpha_j)^2 + c_j = c_1 = c_2 = \frac{2N}{P_u + 2N} \ . \tag{C.78}$$

Hereafter, the details of the proof.

Table C.1: Optimal DPC parameter for the CD-DPC.

$A_1 = A_2$	$B_1 = B_2$		α_1
	$B_1 \neq B_2$ $\lvert c_1 - c_2 \rvert > A(\alpha_1 - \alpha_2)^2$		α_2
	$B_1 \neq B_2$ $\lvert c_1 - c_2 \rvert \leq A(\alpha_1 - \alpha_2)^2$		$\frac{D_1 - D_2}{2(B_1 - B_2)}$
$A_1 \neq A_2$	$\Delta < 0$		α_2
	$\Delta = 0$		α_2
	$\Delta > 0$ $\lvert c_1 - c_2 \rvert \leq$ $\min(A_1, A_2)(\alpha_1 - \alpha_2)^2$		$\alpha_1 + \frac{A_2\lvert\alpha_1 - \alpha_2\rvert - \sqrt{\Delta}}{A_1 - A_2}$
	$\Delta > 0$ $\lvert c_1 - c_2 \rvert >$ $\min(A_1, A_2)(\alpha_1 - \alpha_2)^2$		α_2

First, note that since $A_1 = A_2$, then we can write that:

$$h_{j,v}^2 = \frac{h_{j,v}^2 P_u + N}{P_u + 2N} \ . \tag{C.79}$$

As such, we can say that: $h_{1,v}h_{2,v} \neq 0$. More over, all quantities write then as:

$$A_1 = A_2 = A \triangleq \frac{P_v}{P_u}\frac{P_u + 2N}{P + 2N} \ , \tag{C.80}$$

$$\alpha_j = \frac{P_u}{P_u + 2N}\frac{h_{j,u}}{h_{j,v}} \ , \tag{C.81}$$

$$B_j = P_v \frac{h_{j,u}h_{j,v}}{h_{j,u}^2 P_u + h_{j,v}^2 P_v + N} = \frac{P_v}{P + 2N}\frac{h_{j,u}}{h_{j,v}} \ , \tag{C.82}$$

$$D_j = \frac{h_{j,v}^2 P_v + N}{h_{j,u}^2 P_u + h_{j,v}^2 P_v + N} = \frac{h_{j,v}^2 P_v + N}{h_{j,v}^2 (P + 2N} \ . \tag{C.83}$$

Now, we have that:

$$B_1 = B_2 \Leftrightarrow P_v \left(\frac{h_{1,u}}{h_{1,v}} - \frac{h_{2,u}}{h_{2,v}}\right) = 0 \ , \tag{C.84}$$

$$\Leftrightarrow P_v = 0 \quad \text{or} \quad \cos(\theta_u)\sin(\theta_v) - \cos(\theta_v)\sin(\theta_u) = 0 \ , \tag{C.85}$$

$$\Leftrightarrow P_v = 0 \quad \text{or} \quad \sin(\theta_u - \theta_v) = 0 \ , \tag{C.86}$$

$$\Leftrightarrow P_v = 0 \quad \text{or} \quad \theta_u = \theta_v[\pi] \ , \tag{C.87}$$

but since $\cos^2(\theta_v) = \dfrac{\cos^2(\theta_u)P_u + N}{P_u + 2N}$, then, one can write that:

$$B_1 = B_2 \text{ and } A_1 = A_2 \qquad \Rightarrow \qquad P_v = 0 \text{ or } \cos^2(\theta_u) = \frac{1}{2} \ . \tag{C.88}$$

This implies then that:

$$c_1 = c_2 = \frac{P_v + 2N}{P + 2N} \ , \tag{C.89}$$

$$\alpha_1 = \alpha_2 = \pm\frac{P_u}{P_u + 2N} \ . \tag{C.90}$$

Thus in both cases of $P_v = 0$ and $P_v \neq 0$, the optimal solution is given by:

$$\min_{\alpha}\max_{j=1,2} A_j(\alpha - \alpha_j)^2 + c_j = c_1 = c_2 = \frac{2N}{P_u + 2N} \ . \tag{C.91}$$

Note that, since $\theta_u = \theta_v[\pi]$, then $2\theta_u = 2\theta_v[2\pi]$, thus $s_u = s_v$.
Thus, as for the rate of user 2, two cases unfold:

- Case of $s_u = s_v = 1$, which corresponds to $B_u = \mathbf{h}_{1,2}$, and in this case B_v is co-linear to $\mathbf{h}_{1,2}$ and thus orthogonal to user 2's channel $\mathbf{g}$ leading to a zero achievable rate:

$$R_2 = 0 \ . \tag{C.92}$$

  The power optimization of this point will yields the single capacity point $(C_1, 0)$.

- Case of $s_u = s_v = -1$, which corresponds to $B_u \perp \mathbf{h}_{1,2}$, and in this case B_v is co-linear to user 2's channel $\mathbf{g}$ leading to the achievability of all rate pairs satisfying:

$$\begin{cases} R_1 & \leq & \frac{1}{2}\log_2\left(\frac{P_u+2N}{2N}\right) , \\ R_2 & \leq & \frac{1}{2}\log_2\left(\frac{P+N}{P_u+N}\right) . \end{cases} \tag{C.93}$$

The set of rate pairs obtained can be shown to perform worse than time sharing as is explained hereafter. To show this, let $\alpha \in [0:1]$ such that:

$$R_1 = \frac{1}{2}\log_2\left(\frac{P_u+2N}{2N}\right) = \frac{\alpha}{2}\log_2\left(\frac{P+2N}{2N}\right) . \tag{C.94}$$

We need to show that:

$$R_2 = \frac{1}{2}\log_2\left(\frac{P+N}{P_u+N}\right) \leq \frac{(1-\alpha)}{2}\log_2\left(\frac{P+N}{N}\right) . \tag{C.95}$$

To see this, note that:

$$\frac{P_u+2N}{2N} = \frac{(P+2N)^\alpha}{(2N)^\alpha} \Rightarrow \frac{P_u}{N}+1 = 2\left(\frac{P}{2N}+1\right)^\alpha - 1 \tag{C.96}$$

$$\Rightarrow R_2 = \frac{1}{2}\log_2\left(\frac{\frac{P}{N}+1}{2\left(\frac{P}{2N}+1\right)^\alpha - 1}\right) \tag{C.97}$$

$$\overset{(a)}{\Rightarrow} R_2 \leq \frac{1}{2}(1-\alpha)\log_2\left(\frac{P+N}{N}\right) , \tag{C.98}$$

where (a) is a result of that the function:

$$\begin{array}{rcl} [1:\infty[& \mapsto & \mathbb{R} \\ x & \mapsto & 2(x+1)^\alpha - 1 - (2x+1)^\alpha \end{array} \tag{C.99}$$

by a quick function study, is positive. And thus:

$$2\left(\frac{P}{2N}+1\right)^\alpha - 1 \geq \left(\frac{P}{N}+1\right)^\alpha , \tag{C.100}$$

which proves our claim.

To end the discussion of this case, it turns out that the optimal points obtained are the two single capacity points $(C_1, 0)$ and $(0, C_2)$.

C.5.2 Case of $A_1 = A_2 = A$ and $B_1 \neq B_2$ and $|c_1 - c_2| \leq A(\alpha_1 - \alpha_2)^2$

In this case, the optimal solution of the problem (C.77) is given by:

$$\alpha_{opt} = \frac{D_2 - D_1}{2(B_2 - B_1)} = \frac{c_2 - c_1}{2(\alpha_2 - \alpha_1)} + \frac{1}{2}(\alpha_2 + \alpha_1) . \tag{C.101}$$

Thus, the minimum value of the function to optimize in (C.70) is given by:

$$F_{opt} \triangleq \frac{(c_2 - c_1)^2}{4A(\alpha_2 - \alpha_1)^2} + \frac{1}{2}(c_2 + c_1) + \frac{A}{4}(\alpha_2 - \alpha_1)^2 \ , \tag{C.102}$$

where as for previously:

$$A = \frac{P_v}{P_u}\frac{P_u + 2N}{P + 2N} \ , \tag{C.103}$$

$$c_j = \frac{N}{P_u + 2N}\frac{1}{h_{j,v}^2} \ , \tag{C.104}$$

$$\alpha_j = \frac{P_u}{P_u + 2N}\frac{h_{j,u}}{h_{j,v}} \ . \tag{C.105}$$

After some analytic manipulations we end up with the following expression of the optimal solution:

$$F_{opt} = \frac{1}{(P_u + 2N)\sin^2(2\theta_v)}\left[\frac{N^2(P + 2N)}{P_u P_v}\frac{\cos^2(2\theta_v)}{\sin^2(\theta_u - \theta_v)} + \frac{P_u P_v}{P + 2N}\sin^2(\theta_u - \theta_v) + 2N\right] \ , \tag{C.106}$$

Now, using the fact that:

$$\cos^2(\theta_v) = \frac{\cos^2(\theta_u)P_u + N}{P_u + 2N} \ , \tag{C.107}$$

we can write that:

$$\cos(2\theta_v) = \frac{P_u}{P_u + 2N}\cos(2\theta_u) \ , \tag{C.108}$$

which implies

$$\sin(2\theta_u) = s_u\sqrt{1 - \cos^2(2\theta_u)} = s_u\sqrt{1 - \frac{(P_u + 2N)^2}{P_u^2}\cos^2(2\theta_v)} \ , \tag{C.109}$$

where we recall that:

$$s_u = \frac{\sin(2\theta_u)}{|\sin(2\theta_u)|} \text{ and } \ s_v = \frac{\sin(2\theta_v)}{|\sin(2\theta_v)|} \ . \tag{C.110}$$

In the sequel, we define the two variables:

$$x \triangleq \cos^2(2\theta_v) \ , \tag{C.111}$$

$$a \triangleq \frac{(P_u + 2N)^2}{P_u^2} \ . \tag{C.112}$$

As defined, and recalling (C.108), we can conclude that x lies in the set $\left[0 : \frac{1}{a}\right]$. To further simplify (C.106), we need to express the following quantity:

$$\sin^2(\theta_u - \theta_v) = \frac{1}{2P_u}\left[P_u\left(1 - x - s_u s_v\sqrt{(1 - x)\left(1 - \frac{(P_u + 2N)^2}{P_u^2}x\right)}\right) - 2Nx\right] \ . \tag{C.113}$$

Letting then:

$$\begin{aligned} g(x, s_u, s_v) &\triangleq 2P_u \sin^2(\theta_u - \theta_v) \\ &= P_u \left(1 - x - s_u s_v \sqrt{(1-x)\left(1 - \frac{(P_u + 2N)^2}{P_u^2} x\right)}\right) - 2Nx \ , \end{aligned} \tag{C.114}$$

one ends up with the following optimal function expressed in x, s_u and s_v:

$$F_{opt}(x) = \frac{1}{(1-x)} \left[\frac{2N^2(P+2N)}{P_v} \frac{x}{g(x, s_u, s_v)} + \frac{P_v}{2(P+2N)} g(x, s_u, s_v) + 2N \right] \ . \tag{C.115}$$

Now, the rate of the second user is given by:

$$R_2 = \log_2 \frac{1}{2} \left(1 + \frac{g_v^2 P_v}{g_u^2 P_u + 2N}\right) \ . \tag{C.116}$$

Then, we express:

$$g_v^2 = \cos^2\left(\theta_v + \frac{\pi}{4}\right) = \frac{1 - \sin(2\theta_v)}{2} \tag{C.117}$$

$$= \frac{1 - s_v\sqrt{1-x}}{2} \ . \tag{C.118}$$

Similarly, we can show that:

$$g_u^2 = \frac{1}{2} - \frac{s_u}{2} \sqrt{1 - \frac{(P_u + 2N)^2}{P_u^2} x} \ , \tag{C.119}$$

Thus, the overall optimization problem is given as:

$$\bigcup_{(x, s_u, s_v) \in \mathcal{S}} \left\{ \begin{array}{rcl} R_1 & \leq & \frac{1}{2} \log_2 \left(\frac{1}{F_{opt}(x, s_u, s_v)} \right) \ , \\ R_2 & \leq & \frac{1}{2} \log_2 \left(1 + \frac{P_v(1 - s_v\sqrt{1-x})}{P_u\left(1 - s_u\sqrt{1-ax}\right) + N} \right) \ , \end{array} \right. \tag{C.120}$$

where we define the optimization $\mathcal{S}$ as:

$$\mathcal{S} \triangleq \left\{ x \in \left[0 : \frac{1}{a}\right] \ , \ (s_u, s_v) \in \{-1, 1\}^2 \ , \ \text{s.t} \quad s_u s_v = 1 \Rightarrow x \neq 0 \right\} , \tag{C.121}$$

Hereafter, we study two distinct cases: $s_u s_v = -1$ and $s_u s_v = 1$.

$s_u s_v = +1$

we show in the following section that this case is impossible because $s_u s_v = +1$ contradicts the existence of x such that

$$|c_1 - c_2| \leq A(\alpha_1 - \alpha_2)^2 \ ,$$

$s_u s_v = -1$

When $s_u s_v = -1$, we express the first derivative of the function F_{opt} and show that it is always positive, leading us to the claim that F_{opt} is strictly increasing. Thus, the rate of user 1, R_1 is decreasing in x.

If $s_u = 1$ and $s_v = -1$, then R_2 is easily shown to be decreasing in x, and thus, the optimal rate pair that is achievable is given by $x = 0$ leading thus to:

$$\begin{cases} R_1 & \leq & \frac{1}{2}\log_2\left(\frac{P+2N}{P_v+2N}\right) , \\ R_2 & \leq & \frac{1}{2}\log_2\left(\frac{P_v+N}{N}\right) . \end{cases} \tag{C.122}$$

If $s_u = 1$ and $s_v = -1$, then we can show that R_2 can not be greater than: $\log_2\left(\frac{P_v+N}{N}\right)$, and thus, the achievable rate region is dominated by (C.122).

To see this, note that: R_2 is strictly increasing in x and thus, its maximum value is attained for $x = \frac{1}{a}$. Then, one can easily check that:

$$R_2 = \frac{1}{2}\log_2\left(1 + P_v\frac{1-\sqrt{\frac{4N(P_u+N)}{P_u^2}}}{P_u+2N}\right) \tag{C.123}$$

$$\leq \frac{1}{2}\log_2\left(1+P_v\frac{1}{P_u+2N}\right) \tag{C.124}$$

$$\leq \frac{1}{2}\log_2\left(1+\frac{P_v}{N}\right) , \tag{C.125}$$

which proves our claim.

Thus, the overall obtained rate region for this case, does not outperform the second corner point of CD-DPC, which is already included in the first corner point.

C.5.3 Case of $A_1 = A_2 = A$ and $B_1 \neq B_2$ and $|c_1 - c_2| > A(\alpha_1 - \alpha_2)^2$

In this case, we show that the obtained rate region does not outperform time sharing.

To this end, we start by expressing the following:

$$|c_1 - c_2| > A(\alpha_1-\alpha_2)^2 \qquad \Leftrightarrow \qquad N|\cos(2\theta_v)| > \frac{P_v P_u}{P+2N}\sin^2(\theta_u-\theta_v) . \tag{C.126}$$

With the previous notations of the function g and $x = \cos^2(2\theta_v)$, we can rewrite this condition as:

$$N\sqrt{x} > \frac{P_v}{2(P+2N)}g(x) . \tag{C.127}$$

If $s_u s_v = 1$, then we can show easily that the above condition is always verified even with $P_v \neq 0$ and $x \neq 0$. To see this note that for $x \in [0 : 1/a]$:

$$g(x) = P_u(1-x-\sqrt{(1-x)(1-a\star x)})-2Nx \leq P_u(1-x-1+ax)-2Nx \triangleq h(x) . \tag{C.128}$$

Then, it is easy to show that for $x \in [0 : 1/a]$:

$$N\sqrt{x} \geq h(x) \ , \tag{C.129}$$

since h is linear and $h(0) = 0$ and $h(1/a) = g(1/a) < N\sqrt{1/a}$. Fig. C.1 illustrates clearly our claim.

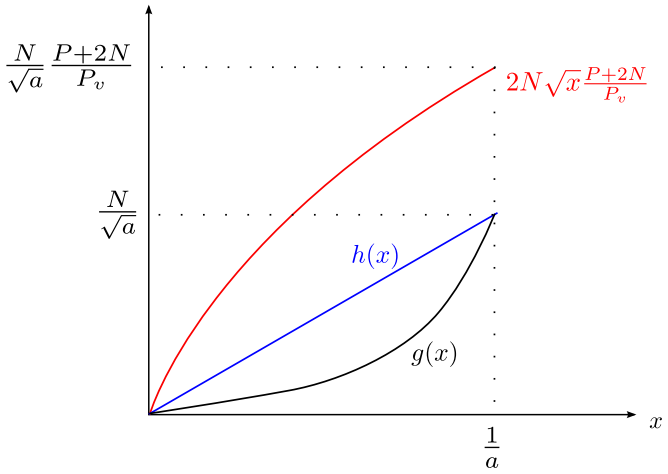


Figure C.1: Comparison of the functions h, g and target upper bound.

Thus, since the condition is always verified, the optimal solution is given by the rate pairs (R_1, R_2) satisfying:

$$\begin{aligned} R_1 &\leq \frac{1}{2}\log_2\left(\frac{P_u + 2N}{2N}(1-\sqrt{x})\right) \ , \\ R_2 &\leq \frac{1}{2}\log_2\left(1 + P_v\frac{1 - s_v\sqrt{1-x}}{P_u(1 - s_u\sqrt{1-ax}) + 2N}\right) \ . \end{aligned} \tag{C.130}$$

If $s_u = s_v = -1$, then we show that the obtained rate region is included in the time sharing rate region. To this end, we choose to show this claim on a larger rate region given by:

$$\begin{cases} R_1 &\leq \frac{1}{2}\log_2\left(\frac{P_u + 2N}{2N}(1-x)\right) \ , \\ R_2 &\leq \frac{1}{2}\log_2\left(1 + P_v\frac{1 - s_v\sqrt{1-x}}{P_u(1 - s_u\sqrt{1-ax}) + 2N}\right) \ . \end{cases} \tag{C.131}$$

We proceed as follows to show that the obtained rate region for fixed P_u, P_v and N, is concave.

Let $\alpha \in [0 : 1]$, such that:

$$\frac{1}{2}\log_2\left(\frac{P_u + 2N}{2N}(1-x)\right) \triangleq \alpha\log_2\left(\frac{P_u + 2N}{2N}\right) + (1-\alpha)\log_2\left(\frac{P_u + 2N}{2N}\left(1 - \frac{1}{a}\right)\right) \ . \tag{C.132}$$

Thus, we can show that:

$$1 - x = \left(1 - \frac{1}{a}\right)^{1-\alpha} \ . \tag{C.133}$$

Thus, letting $y \triangleq \left(1 - \frac{1}{a}\right)$, the previous rate of user 2 writes as:

$$R_2 \leq \frac{1}{2}\log_2\left(1 + P_v\sqrt{1-y}\frac{1+\sqrt{y^{1-\alpha}}}{P_u\left(1+\sqrt{y^{1-\alpha}-y}\right)}\right) \triangleq \frac{1}{2}\log_2\left(f(\alpha)\right) \ . \tag{C.134}$$

Our aim is to show that R_2 is convex in α, thus, we need to show that:

$$f''(\alpha)f(\alpha) - (f'(\alpha))^2 \geq 0 \ . \tag{C.135}$$

We have that:

$$f'(\alpha) = \frac{P_v\log(y)\sqrt{1-y}}{2P_u\left(1+\sqrt{y^{1-\alpha}-y}\right)^2}\left(-\sqrt{y^{1-\alpha}} + \frac{\sqrt{y^{1-\alpha}}+y}{\sqrt{1-y^\alpha}}\right) \ . \tag{C.136}$$

It is easy to see that thus R_2 is decreasing in α since $\log(y) \leq 0$.

As for the second derivative, one can show that it writes as:

$$f''(\alpha) = \frac{P_v\log^2(y)\sqrt{1-y}}{4P_u(1-y^\alpha)\sqrt{1-y^\alpha}}\frac{1}{\left(1+\sqrt{y^{1-\alpha}-y}\right)^3}G(\alpha) \ , \tag{C.137}$$

where $G(\alpha)$ is given by:

$$\begin{aligned} G(\alpha) = {} & 2\sqrt{y^{1-\alpha}-y}\left(\sqrt{y^{1-\alpha}}(1-\sqrt{1-y^\alpha})+y\right) \\ & +(1+\sqrt{y^{1-\alpha}-y})\left((1-y^\alpha)\sqrt{y^{1-\alpha}}(\sqrt{1-y^\alpha}-1)+y^\alpha(y+\sqrt{y^{1-\alpha}})\right) \end{aligned} \tag{C.138}$$

Showing that R_2 is convex in α, i.e showing that (C.135) holds, amounts then to showing that:

$$\frac{P_v(1+\sqrt{y^{1-\alpha}})\sqrt{1-y} + P_u(1+\sqrt{y^{1-\alpha}-y})}{\sqrt{1-y^\alpha}\sqrt{1-y}}G(\alpha) \geq P_v\left(\sqrt{y^{1-\alpha}}(1-\sqrt{1-y^\alpha})+y\right)^2 \ . \tag{C.139}$$

We show the stronger result that consists in:

$$\frac{G(\alpha)}{\sqrt{1-y^\alpha}} \geq \left(\sqrt{y^{1-\alpha}}(1-\sqrt{1-y^\alpha})+y\right)^2 \ , \tag{C.140}$$

which would yield the desired inequality.

Note here that since:

$$\begin{aligned} (1-y^\alpha)\sqrt{y^{1-\alpha}}(\sqrt{1-y^\alpha}-1) + y^\alpha(y+\sqrt{y^{1-\alpha}}) & \\ \geq \sqrt{y^{1-\alpha}}(\sqrt{1-y^\alpha}-1) + y^\alpha(y+\sqrt{y^{1-\alpha}}) & \quad \text{(C.141)} \\ \geq \sqrt{y^{1-\alpha}}(1-y^\alpha-1) + y^\alpha(y+\sqrt{y^{1-\alpha}}) & \quad \text{(C.142)} \\ \geq 0 \ , & \quad \text{(C.143)} \end{aligned}$$

then,

$$G(\alpha) \geq 2\sqrt{y^{1-\alpha}-y}\left(\sqrt{y^{1-\alpha}}(1-\sqrt{1-y^{\alpha}})+y\right) \ . \tag{C.144}$$

Hence ,we can write:

$$\begin{aligned} G(\alpha) - \sqrt{1-y^{\alpha}}&\left(\sqrt{y^{1-\alpha}}(1-\sqrt{1-y^{\alpha}})+y\right)^2 \\ &\geq \sqrt{1-y^{\alpha}}\left(\sqrt{y^{1-\alpha}}(1-\sqrt{1-y^{\alpha}})+y\right)\left(\sqrt{y^{1-\alpha}}(1+\sqrt{1-y^{\alpha}})+y\right) \quad \text{(C.145)} \\ &\geq 0 \ , \quad \text{(C.146)} \end{aligned}$$

this ends thus the proof. Thus, R_2 being convex in α and R_1 linear in α the trajectory of $R_2(R_1)$ describes then a concave rate region.

If $s_u = s_v = 1$, we show that the obtained rate region is included in a suboptimal rate region compared to time sharing, studied earlier and given by:

$$\begin{cases} R_1 & \leq & \frac{1}{2}\log_2\left(\frac{P_u+2N}{2N}\right) \ , \\ R_2 & \leq & \frac{1}{2}\log_2\left(\frac{P+N}{P_u+N}\right) \ . \end{cases} \tag{C.147}$$

To show this, note that the bound on R_1 is trivial. However, concerning the second user's rate, note that as it writes:

$$R_2 = \frac{1}{2}\log_2\left(1+P_v\frac{1-\sqrt{1-x}}{P_u(1-\sqrt{1-ax})+2N}\right) \triangleq \log_2\left(1+g(x)\right) \ , \tag{C.148}$$

R_2 is not always strictly monotonic. The sign of its first derivative in x is given by the sign of g':

$$(P_u+2N)\sqrt{1-ax}+P_u(a-1-a\sqrt{1-x}) \ , \tag{C.149}$$

that depends on the respective values of P_u and N. If there exists any point for which the first derivative is null x_{opt}, then it will imply that:

$$\begin{aligned} P_u\left(1-\sqrt{1-ax}\right)+2N=&(P_u+2N)\left(1-\sqrt{1-x}+1-\frac{1}{a}\right) \quad \text{(C.150)} \\ \geq&(P_u+2N)\left(1-\sqrt{1-x}\right)\geq 0 \ . \quad \text{(C.151)} \end{aligned}$$

Then, we can conclude that:

$$R_2 \leq \frac{1}{2}\log_2\left(1+\frac{P_v}{P_u+2N}\right) \ . \tag{C.152}$$

It no such point exists such that $g'(x) = 0$, then R_2 is increasing in x and thus, the maximum value is obtained for $x = 1/a$, which clearly yields to the desired bound on R_2.

Now, if $s_u s_v = -1$, then two cases unfold following the signs of s_u and s_v. In both cases, the obtained rate region is shown not to outperform the optimal rate region we claim. If $s_u = -1$ and $s_v = 1$, then, we can show that the rate region:

$$\begin{cases} R_1 & \leq & \frac{1}{2}\log_2\left(\frac{P_u+2N}{2N}(1-\sqrt{x})\right) \leq \frac{1}{2}\log_2\left(\frac{P_u+2N}{2N}\right) \ , \\ R_2 & \leq & \frac{1}{2}\log_2\left(1+P_v\frac{1-\sqrt{1-x}}{P_u(1+\sqrt{1-ax})+2N}\right) \leq \frac{1}{2}\log_2\left(\frac{P+2N}{P_u+2N}\right) \ , \end{cases} \tag{C.153}$$

is included in the sub-optimal rate region given by (C.93) which in turn does not outperform time sharing.

On the other side, if $s_u = 1$ and $s_v = -1$, then we will show that the second corner point of CD-DPC inner bound contains the obtained rate region. In this case, it can be easily shown that both R_1 and R_2 are decreasing in x. However, not all values of x are admissible due to the constraint.

Let us start by characterizing the set of values such that:

$$N\sqrt{x} > \frac{P_v}{2(P+2N)}\left(P_u(1-x+\sqrt{(1-x)(1-ax)})-2Nx\right) \ . \tag{C.154}$$

As done previously, we will solve only the simpler problem that yields a larger solution set and that is illustrated in Fig. C.2:

$$N\sqrt{x} > \frac{P_v}{2(P+2N)}\left(P_u(1-x+1-ax)-2Nx\right) \ . \tag{C.155}$$

Solving this problem yields the following value of the infinimum of all admissible beam

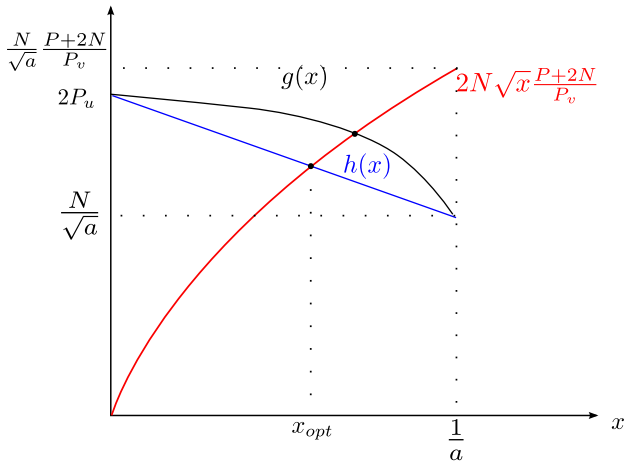


Figure C.2: Comparison of the functions h, g and target upper bound.

directions:

$$x_{opt} = \frac{P_u^2}{2(P_u+N)^2(P_u+2N)^2}\left[2(P_u+N)(P_u+2N)+\frac{N^2(P+2N)^2}{P_v^2}\right.$$
$$\left.-\frac{N(P+2N)}{P_v}\sqrt{\frac{N^2(P+2N)^2}{P_v^2}+4(P_u+N)(P_u+2N)}\right] \tag{C.156}$$

Since the solution of problem (C.155) yields a smaller value of the inf of admissible solutions, the resulting rate region is wider. However, we show that it still remains included in the second corner point of MD-DPC inner bound given by

$$\begin{cases} R_1 & \leq & \frac{1}{2}\log_2\left(\frac{P+2N}{P_u+2N}\right) \ , \\ R_2 & \leq & \frac{1}{2}\log_2\left(\frac{P_v+N}{N}\right) \ . \end{cases} \tag{C.157}$$

The bound on the rate R_2 is quite trivial and requires no further proof. However, the bound on rate R_1 requires showing that:

$$x_{opt} \geq \frac{P_u^2 P_v^2}{(P_u + 2N)^2 (P_v + 2N)^2} \ , \tag{C.158}$$

which can be shown through evolved bounding techniques. As a conclusion for these cases, no rate region outperforms the second corner point of CD-DPC inner bound.

C.5.4 case of $A_1 \neq A_2$ and $(B_1 - B_2)^2 = (A_1 - A_2)(D_1 - D_2)$

In this case, we start by showing that the above condition imposes:

$$\theta_u = \theta_v[\pi] \ . \tag{C.159}$$

Let us first quickly denote:

$$K_{Y_1} \triangleq \cos^2(\theta_u) P_u + \cos^2(\theta_v) P_v + N \ , \tag{C.160}$$
$$K_{Y_2} \triangleq \sin^2(\theta_u) P_u + \sin^2(\theta_v) P_v + N \ . \tag{C.161}$$

Next, recall that:

$$B_1 = \frac{P_v \cos(\theta_u)\cos(\theta_v)}{\cos^2(\theta_u) P_u + \cos^2(\theta_v) P_v + N} = \frac{P_v \cos(\theta_u)\cos(\theta_v)}{K_{Y_1}} \ , \tag{C.162}$$
$$B_2 = \frac{P_v \sin(\theta_u)\sin(\theta_v)}{\sin^2(\theta_u) P_u + \sin^2(\theta_v) P_v + N} = \frac{P_v \sin(\theta_u)\sin(\theta_v)}{K_{Y_2}} \ , \tag{C.163}$$
$$A_1 = \frac{P_v}{P_u} \frac{\cos^2(\theta_u) P_u + N}{K_{Y_1}} = \frac{P_v}{P_u} \left(1 - \frac{\cos^2(\theta_v) P_v}{K_{Y_1}} \right) \ , \tag{C.164}$$
$$A_2 = \frac{P_v}{P_u} \frac{\sin^2(\theta_u) P_u + N}{K_{Y_2}} = \frac{P_v}{P_u} \left(1 - \frac{\sin^2(\theta_v) P_v}{K_{Y_2}} \right) \ , \tag{C.165}$$
$$D_1 = \frac{\cos^2(\theta_v) P_v + N}{K_{Y_1}} = \left(1 - \frac{\cos^2(\theta_u) P_u}{K_{Y_1}} \right) \ , \tag{C.166}$$
$$D_2 = \frac{\sin^2(\theta_v) P_v + N}{K_{Y_2}} = \left(1 - \frac{\sin^2(\theta_u) P_u}{K_{Y_2}} \right) \ . \tag{C.167}$$

And that $A_1 \neq A_2 \Rightarrow P_v \neq 0$. Thus,

$$\begin{aligned}
&(B_1 - B_2)^2 = (A_1 - A_2)(D_1 - D_2) \\
\Leftrightarrow &\left(\frac{\cos(\theta_u)\cos(\theta_v)}{K_{Y_1}} - \frac{\sin(\theta_u)\sin(\theta_v)}{K_{Y_2}} \right)^2 \\
= &\left(\frac{\sin^2(\theta_v)}{K_{Y_2}} - \frac{\cos^2(\theta_v)}{K_{Y_1}} \right) \left(\frac{\sin^2(\theta_u)}{K_{Y_2}} - \frac{\cos^2(\theta_u)}{K_{Y_1}} \right) && \text{(C.168)} \\
\Leftrightarrow &K_{Y_1} K_{Y_2} \left(\sin(\theta_v)\cos(\theta_u) - \sin(\theta_u)\cos(\theta_v) \right)^2 = 0 && \text{(C.169)} \\
\Leftrightarrow &K_{Y_1} K_{Y_2} \sin^2(\theta_u - \theta_v) = 0 && \text{(C.170)}
\end{aligned}$$

$$\Leftrightarrow \theta_u = \theta_v[\pi] \ . \tag{C.171}$$

The optimal solution of the system (C.74), is then given by:

$$R_1 = \log_2\left(\frac{\min(\sin^2(\theta_v), \sin^2(\theta_v))P_u + N}{N}\right) \tag{C.172}$$

$$= \log_2\left(\frac{(1 - |\cos(2\theta_v)|)P_u + 2N}{2N}\right) \tag{C.173}$$

$$\leq \log_2\left(\frac{(1 - \sqrt{\cos^2(2\theta_v)})P_u + 2N}{2N}\right) \ , \tag{C.174}$$

define then:

$$x \triangleq \cos^2(2\theta_v) \ . \tag{C.175}$$

On the other side, note that:

$$R_2 = \log_2\left(\frac{\cos^2(\theta_v + \pi/4)P + N}{\cos^2(\theta_v + \pi/4)P_u + N}\right) \tag{C.176}$$

$$= \log_2\left(\frac{\sin(2\theta_v)P + 2N}{\sin(2\theta_v)P_u + 2N}\right) \tag{C.177}$$

$$\leq \log_2\left(\frac{(1 - s_v\sqrt{1-x})P + 2N}{(1 - s_v\sqrt{1-x})P_u + 2N}\right) \ , \tag{C.178}$$

if $s_v = -1$, then R_2 is decreasing in x, and thus the optimal value is given by:

$$R_2 = \log_2\left(\frac{P + 2N}{P_u + 2N}\right) \ . \tag{C.179}$$

And since:

$$R_1 \leq \log_2\left(\frac{P_u + 2N}{2N}\right) \ , \tag{C.180}$$

then the obtained region is included in the set of rate pairs such that:

$$\begin{cases} R_1 \ \leq \ \log_2\left(\dfrac{P_u + 2N}{2N}\right) \ , \\ R_2 \ \leq \ \log_2\left(\dfrac{P + 2N}{P_u + 2N}\right) \ . \end{cases} \tag{C.181}$$

which was shown to perform less than time sharing. Now, if $s_v = 1$, then R_2 is increasing in x where $x \in [0:1]$, and hence, the maximum is obtained for $x = 1$, which yields the same rate of user 2. For similar reasons, the obtained rate pair does not outperform time sharing.

Thus, the overall rate region obtained in this case, is included in mere time sharing.

C.5.5 case of $A_1 \neq A_2$ and $(B_1 - B_2)^2 < (A_1 - A_2)(D_1 - D_2)$

Since we have that:

$$(B_1 - B_2)^2 - (A_1 - A_2)(D_1 - D_2) = \frac{Pv^2}{K_{Y_1}K_{Y_2}}\left(\sin(\theta_v - \theta_u)\right)^2 \ , \tag{C.182}$$

having $(B_1 - B_2)^2 < (A_1 - A_2)(D_1 - D_2)$ is impossible.

C.5.6 case of $A_1 \neq A_2$, $(B_1-B_2)^2 > (A_1-A_2)(D_1-D_2)$ and $|c_1-c_2| \leq \min(A_1, A_2)(\alpha_1 - \alpha_2)^2$

In this case, we can show that, the two possible optimum solutions are obtained for $\theta_u = \pi/4$ or $\theta_u = -\pi/4$.

The case where $\theta_u = \pi/4$ is the claimed optimal rate region. As for the case where $\theta_u = -\pi/4$, the resulting rate region consists of all rate pairs satisfying:

$$\begin{cases} R_1 & \leq & \frac{1}{2}\log_2\left(\frac{P_u+2N}{\frac{1+y}{P_uP_v\frac{1+y}{P+2N+\sqrt{P+2N+(y^2-1)P_v}}+2N}}\right) , \\ R_2 & \leq & \frac{1}{2}\log_2\left(1+P_v\frac{1-y}{2(P_u+N)}\right) . \end{cases} \tag{C.183}$$

Note, that in this case, the maximum is achieved at both rates letting $y = -1$, thus, the resulting rate region can not outperform the rate region given by:

$$\begin{cases} R_1 & \leq & \frac{1}{2}\log_2\left(\frac{P_u+2N}{2N}\right) , \\ R_2 & \leq & \frac{1}{2}\log_2\left(\frac{P+N}{P_u+N}\right) , \end{cases} \tag{C.184}$$

which was clearly shown not to outperform time-sharing.

C.5.7 case of $A_1 \neq A_2$, $(B_1-B_2)^2 > (A_1-A_2)(D_1-D_2)$ and $|c_1-c_2| > \min(A_1, A_2)(\alpha_1 - \alpha_2)^2$

In this peculiar last case, we show that the obtained rate region can not exceed time sharing neither. In this case, the resulting rate region writes as:

$$\begin{cases} R_1 & \leq & \frac{1}{2}\log_2\left(\frac{(1-|\cos(2\theta_u)|)P_u+2N}{2N}\right) \\ R_2 & \leq & \frac{1}{2}\log_2\left(1+P_v\frac{(1-s_v\sqrt{1-\cos^2(2\theta_v)})}{P_u(1-s_u\sqrt{1-cos^2(2\theta_u)})+2N}\right) \end{cases} \tag{C.185}$$

The case where $s_u = -1$, then we can show resorting to the same tools used on the analysis of the concavity in the previous sections that the obtained rate region when $\cos^2(2\theta_u)$spans the interval $[0:1]$, is concave for every value of $\cos^2(2\theta_v)$, thus, the resulting union can be at most concave. When $s_u = 1$, two cases unfold and R_1 and R_2 are both decreasing in $\cos^2(2\theta_u)$, and for a fixed beam direction $\mathbf{B}_v$, the optimal rate pair is given by:

$$\begin{cases} R_1 & \leq & \frac{1}{2}\log_2\left(\frac{P_u+2N}{2N}\right) , \\ R_2 & \leq & \frac{1}{2}\log_2\left(1+P_v\frac{(1-s_v\sqrt{1-\cos^2(2\theta_v)})}{2N}\right) . \end{cases} \tag{C.186}$$

C.6 Proof of Achievability of $\mathcal{R}_{3-ARV}$

We fix a pmf $p_{QU_1U_2VX}$. Let R_0, R_1, R_2 denote the message rates and $T_{1,2}, T_{1,1}$ and T_2 denote the binning rates. Generate $2^{n\,R_0}$ sequences $q^n(w_0)$, $w_0 \in [1 : 2^{n\,R_0}]$ each following the pmf: $\prod_{i=1}^n P_Q(q_i(w_0))$. For each w_0, generate $2^{n\,T_2}$ sequences $v^n(l_2, w_0)$ following the pmf: $\prod_{i=1}^n P_{V|Q}(v_i(l_2, w_0)|q_i(w_0))$ and map them randomly in $2^{n\,R_2}$ bins $B^n(w_2, w_0)$. Generate similarly $2^{n\,T_{1,1}}$ sequences $u_1^n(l_{1,1}, w_0)$ and map them randomly in $2^{n\,R_1}$ bins $B_1^n(w_1, w_0)$ and $2^{n\,T_{1,2}}$ sequences $u_2^n(l_{1,2}, w_0)$ and map them in a distinct set of $2^{n\,R_1}$ bins $B_2^n(w_1, w_0)$.
Encoding: for each message triple (w_0, w_1, w_2) to be transmitted, find in the product of all bins $B^n(w_i, w_0)$, a triple of sequences $u_1^n(l_{1,1}, w_0), u_2^n(l_{1,2}, w_0), v^n(l_1, w_0)$ such that:

$$\Big(q^n(w_0), u_1^n(l_{1,1}, w_0), u_2^n(l_{1,2}, w_0), v^n(l_2, w_0)\Big) \in T_\delta^n(QU_1U_2V)\,.$$

Send then a random mapping sequence: $x^n(w_0, l_{1,1}, l_{1,2}, l_2)$. The encoding is error free if all inequalities in $\mathbb{T}$ are verified.
Decoding: Each receiver decodes its intended messages (w_0, w_j) by decoding the index l_j and non-uniquely the common message, yielding the constraints stated in $\mathcal{M}$.

Appendix D

Proof of results of Chapter 3

D.1 Proof of achievability for the Multicast CIFC

All the channel outputs in the Multicast setting are to be treated in a similar manner, thus, we show the achievability only with one primary channel output Y. Fig. D.1 summarizes the encoding process.

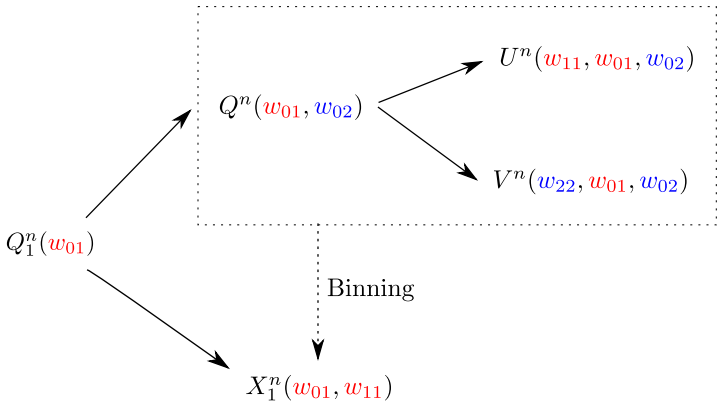


Figure D.1: Encoding for the Cognitive Interference Channel.

Rate splitting:

The message W_1 is split in two parts W_{01} of rate R_{01} that is going to be decoded by all users and a private part W_{11} that is going to be decoded only by user Y.

Codebook generation:

At source 1: First generate $2^{nR_{01}}$ sequences $q_1^n(w_{01})$ following $\prod_{i=1}^n P_{Q_1}(q_{1,i}(w_{01}))$. For each sequence $q_1^n(w_{01})$, generate $2^{nR_{11}}$ sequences $x_1^n(w_{11})$ following $\prod_{i=1}^n P_{X_1|Q_1}(x_{1,i}(w_{11}, w_{01}))$.

At Source 2: For each sequence $q_1^n(w_{01})$, generate $2^{n(T_{02})}$ sequences $q^n(w_{01}, s_{02})$ following $\prod_{i=1}^n P_{Q|Q_1}(q_i(w_{01}, s_{02}))$ and throw them in $2^{nR_{02}}$ bins $B_0^n(w_{01}, w_{02})$. For each sequence $q^n(w_{01}, s_{02})$, generate $2^{nT_{11}}$ sequences $u^n(s_{11}, w_{01}, s_{02})$ and $2^{nT_{22}}$ sequences $v^n(s_{22}, w_{01}, s_{02})$ following $\prod_{i=1}^n P_{U|QQ_1}(u_i(s_{11}, w_{01}, s_{02}))$ and $\prod_{i=1}^n P_{V|QQ_1}(v_i(s_{22}, w_{01}, s_{02}))$ and throw them respectively in $2^{nR_{11}}$ bins $B_1^n(w_{11}, w_{01}, s_{02})$ and $2^{nR_{22}}$ bins $B_2^n(w_{22}, w_{01}, s_{02})$.

Encoding:

The encoder 1 sends $x_1^n(w_{11}, w_{01})$. The encoder 2 finds in bin $B_0^n(w_{01}, w_{02})$ a sequence indexed by s_{02} such that

$$(x_1^n(w_{11}, w_{01}), q_1^n(w_{01}), q^n(w_{01}, s_{02})) \in \mathcal{T}^{(n)}_{[QQ_1X_1]} \ . \tag{D.1}$$

Then, it looks in the product bin $B_1^n(w_{22}, w_{01}, s_{02}) \times B_2^n(w_{22}, w_{01}, s_{02})$ for a couple of sequences such that:

$$(x_1^n(w_{11}, w_{01}), q_1^n(w_{01}), q^n(w_{01}, s_{02}), u^n(s_{11}, w_{01}, s_{02}), v^n(s_{22}, w_{01}, s_{02})) \in \mathcal{T}^{(n)}_{[QQ_1UVX_1]} \ . \tag{D.2}$$

It then sends a codeword $x_2^n(s_{11}, s_{22}, w_{01}, s_{02})$.

The encoding will be flawless if the following inequalities hold:

$$T_{02} - R_{02} \geq I(X_1; Q|Q_1) \ , \tag{D.3}$$
$$T_{11} - R_{11} \geq I(U; X_1|Q_1Q) \ , \tag{D.4}$$
$$T_{22} - R_{22} \geq I(V; X_1|Q_1Q) \ , \tag{D.5}$$
$$T_{11} - R_{11} + T_{22} - R_{22} \geq I(U; V|Q_1Q) + I(UV; X_1|Q_1Q) \ . \tag{D.6}$$

Decoding:

Receiver 2 decodes simultaneously the indices (w_{01}, s_{02}, s_{22}) while decoder 1 decodes simultaneously $(w_{01}, s_{02}, w_{11}, s_{11})$. The probability of error can be made arbitrarily small if the following inequalities hold:

$$T_{22} \leq I(V; Z|QQ_1) \ , \tag{D.7}$$
$$T_{02} + T_{22} \leq I(QV; Z|Q_1) \ , \tag{D.8}$$
$$R_{01} + T_{02} + T_{22} \leq I(Q_1QV; Z) \ , \tag{D.9}$$
$$T_{11} \leq I(X_1U; Y|Q) + I(QU; X_1|Q_1) \ , \tag{D.10}$$
$$T_{02} + T_{11} \leq I(X_1QU; Y|Q_1) + I(QU; X_1|Q_1) \ , \tag{D.11}$$
$$R_{01} + T_{02} + T_{11} \leq I(Q_1X_1QU; Y) + I(QU; X_1|Q_1) \ . \tag{D.12}$$

Fourrier Motzkin Elimination:

After running FME on binning rates T_{02}, T_{11}, T_{22} and on rate splitting parameters R_{01} and R_{02}, we end up with the rate region in Theorem 1.

Multicast setting:

All channel output Y_j , $j \in [1 : N]$ perform all the same decoding strategy, thus, the rate region can be written similarly obtained replacing Y with the minimum over all channel outputs Y_j, where $j \in [1 : N]$.

Appendix E

Proof of results of Chapter 4

E.1 Proof of Lemma 3

We want to show the following set of inequalities:

$$I(Q^n; Z^n) \leq n\, I(Q; Z) + n\, \epsilon_n \ , \tag{E.1}$$
$$I(U_1^n; U_2^n | Q^n) \leq n\, I(U_1; U_2 | Q) + n\, \epsilon_n \ , \tag{E.2}$$
$$I(U_1^n U_2^n; Z^n | Q^n) \leq n\, I(U_1 U_2; Z | Q) + n\, \epsilon_n \ . \tag{E.3}$$

All inequalities can be proved using the same approach, so we only prove inequality (E.2).

Let $\mathcal{E}$ be the indicator function defined by

$$\mathcal{E} \triangleq \begin{cases} 1 & \text{if } (q^n, u_1^n, u_2^n) \in T_\delta^n(QU_1U_2) \\ 0 & \text{otherwise} \end{cases} \tag{E.4}$$

with probability $\mathbb{P}(\mathcal{E} = 1)$. We have that:

$$\begin{aligned} I(U_1^n; U_2^n | Q^n) &\leq I(U_1^n, \mathcal{E}; U_2^n | Q^n) && \text{(E.5)} \\ &= I(U_1^n; U_2^n | Q^n, \mathcal{E}) + I(\mathcal{E}; U_2^n | Q^n) && \text{(E.6)} \\ &\overset{(a)}{\leq} I(U_1^n; U_2^n | Q^n, \mathcal{E}) + 1 && \text{(E.7)} \\ &= \mathbb{P}(\mathcal{E} = 1) I(U_1^n; U_2^n | Q^n, \mathcal{E} = 1) + \mathbb{P}(\mathcal{E} = 0) I(U_1^n; U_2^n | Q^n, \mathcal{E} = 0) + 1 && \text{(E.8)} \\ &\leq I(U_1^n; U_2^n | Q^n, \mathcal{E} = 1) + n\, \mathbb{P}(\mathcal{E} = 0) \log_2(\|U_2\|) + 1 \ , && \text{(E.9)} \end{aligned}$$

where (a) is due to upper bounding $h_2(\mathcal{E}) \leq 1$. By the codebook generation, as n grows large, $\mathbb{P}(\mathcal{E} = 0)$ can be made arbitrarily small. Note that if encoding is succeeds, only jointly typical sequences U_1^n and U_2^n are sent. Then, if $\mathcal{E} = 1$, as a result of Lemma 8, we can have

$$I(U_1^n; U_2^n | Q^n, \mathcal{E} = 1) \leq nI(U_1; U_2 | Q) + n\epsilon_n \tag{E.10}$$

and thus,

$$\frac{1}{n} I(U_1^n; U_2^n | Q^n) \leq I(U_1; U_2 | Q) + 2\epsilon_n \ . \tag{E.11}$$

The remaining inequalities follow in a similar manner and thus details are omitted here.

E.2 Proof of Lemma 4

In this section, we want to prove the following:

$$\limsup_{n\to\infty} \frac{1}{n} H(S_0 S_1 S_2 | Z^n \bar{W}_0 \bar{W}_1 \bar{W}_2, \mathcal{C}) \leq \max\{0, I_1, I_2, I_3, I_4\} \ .$$

To do this, given the output z^n and the messages $(\bar{W}_0, \bar{W}_1, \bar{W}_2)$, let us define $\mathcal{S}$ as the set of indices (s_0, s_1, s_2) falling in the respective messages' bins, such that:

$$(q^n(s_0), u_1^n(s_0, s_1), u_2^n(s_0, s_2), z^n) \in T_\delta^n(QU_1U_2Z) \ . \tag{E.12}$$

Then, we can show that the expected size of this list, over all codebooks, is upper bound by

$$\mathbb{E}(\|\mathcal{S}\|) \leq 1 + 2^{nI_1} + 2^{nI_2} + 2^{nI_3} + 2^{nI_4} \ , \tag{E.13}$$

where:

$$I_1 = T_1 - R_1 - I(U_1; ZU_2|Q) \ , \tag{E.14}$$
$$I_2 = T_2 - R_2 - I(U_2; ZU_1|Q) \ , \tag{E.15}$$
$$I_3 = T_1 - R_1 + T_2 - R_2 - I(U_1U_2; Z|Q) - I(U_1; U_2|Q) \ , \tag{E.16}$$
$$I_4 = T_0 - R_0 + T_1 - R_1 + T_2 - R_2 - I(QU_1U_2; Z) - I(U_1; U_2|Q) \ . \tag{E.17}$$

To see this, one can note that:

$$\mathbb{E}\|\mathcal{S}\| = \mathbb{P}\{(S_0, S_1, S_2) \in \mathcal{S}\} + \sum_{(s_0,s_1,s_2)\neq(S_0,S_1,S_2)} \mathbb{P}\{(s_0, s_1, s_2) \in \mathcal{S}\}. \tag{E.18}$$

where (S_0, S_1, S_2) are the true indices chosen by the source.

Due to the LLN and the codebook construction, and Lemma 5, we can show that:

$$\mathbb{P}\{(S_0, S_1, S_2) \in \mathcal{S}\} \geq 1 - \eta \tag{E.19}$$

As for the probability of undetected errors, we can distinguish many cases following the values of (s_0, s_1, s_2). Hereafter, we give only representative classes of errors.

- If $s_1 \neq S_1$ and $(s_0, s_2) = (S_0, S_2)$, then by similar tools to Lemma 8, we can show that:
$$\mathbb{P}\{(S_0, s_1, S_2) \in \mathcal{S}\} \leq 2^{[-nI(U_1;ZU_2|Q)+n\epsilon_n]} \tag{E.20}$$

- If $s_1 \neq S_1$, $s_2 \neq S_2$ and $s_0 = S_0$, then:
$$\mathbb{P}\{(S_0, s_1, s_2) \in \mathcal{S}\} \leq 2^{[-nI(U_1U_2;Z|Q)-nI(U_1;U_2|Q)+n\epsilon_n]} \tag{E.21}$$

- Last, if $s_0 \neq S_0$, then for all (s_1, s_2),
$$\mathbb{P}\{(s_0, s_1, s_2) \in \mathcal{S}\} \leq 2^{[-nI(QU_1U_2;Z)-nI(U_1;U_2|Q)+n\epsilon_n]} \tag{E.22}$$

Now, once the list size has been bounded, by defining

$$\mathcal{E} \triangleq \begin{cases} 1 & \text{if } (S_0, S_1, S_2) \in \mathcal{S} \\ 0 & \text{if otherwise} \end{cases} \tag{E.23}$$

we have that

$$\begin{aligned}
& H(S_0S_1S_2|Z^n\bar{W}_0\bar{W}_1\bar{W}_2, \mathcal{C}) \\
&= I(\mathcal{E}; S_0S_1S_2|Z^n\bar{W}_0\bar{W}_1\bar{W}_2, \mathcal{C}) + H(S_0S_1S_2|Z^n\bar{W}_0\bar{W}_1\bar{W}_2, \mathcal{E}, \mathcal{C}) && \text{(E.24)} \\
&\overset{(a)}{\leq} 1 + H(S_0S_1S_2|Z^n\bar{W}_0\bar{W}_1\bar{W}_2, \mathcal{E}, \mathcal{C}) && \text{(E.25)} \\
&\overset{(b)}{\leq} 1 + H(S_0S_1S_2|Z^n\bar{W}_0\bar{W}_1\bar{W}_2, \mathcal{E}=1, \mathcal{C}) + \mathbb{P}(\mathcal{E}=0)H(S_0S_1S_2|\bar{W}_0\bar{W}_1\bar{W}_2)\ , && \text{(E.26)}
\end{aligned}$$

where (a) comes from that the entropy of the binary variable $\mathcal{E}$ is upper-bounded by 1 while (b) follows by upper bounding: $\mathbb{P}(\mathcal{E}=1) \leq 1$ and

$$H(S_0S_1S_2|Z^n\bar{W}_0\bar{W}_1\bar{W}_2, \mathcal{E}=0, \mathcal{C}) \leq H(S_0S_1S_2|\bar{W}_0\bar{W}_1\bar{W}_2)\ . \tag{E.27}$$

By our codebook construction and Lemma 5, again $\mathbb{P}(\mathcal{E}=0)$ can be made arbitrarily small. Next, note that:

$$\begin{aligned}
& H(S_0S_1S_2|Z^n\bar{W}_0\bar{W}_1\bar{W}_2, \mathcal{E}=1, \mathcal{C}) \\
&\overset{(a)}{=} H(S_0S_1S_2|Z^n\bar{W}_0\bar{W}_1\bar{W}_2, \mathcal{E}=1, \mathcal{C}, \mathcal{S}, \|\mathcal{S}\|) && \text{(E.28)} \\
&\leq H(S_0S_1S_2|\mathcal{E}=1, \mathcal{S}, \|\mathcal{S}\|) && \text{(E.29)} \\
&= \sum_{s\in\text{supp}(\|\mathcal{S}\|)} P(\|\mathcal{S}\|=s)H(S_0S_1S_2|\mathcal{E}=1, \mathcal{S}, \|\mathcal{S}\|=s) && \text{(E.30)} \\
&\overset{(b)}{\leq} \sum_{s\in\text{supp}(\|\mathcal{S}\|)} P(\|\mathcal{S}\|=s)\log_2(s) && \text{(E.31)} \\
&= \mathbb{E}\left[\log_2(\|\mathcal{S}\|)\right] && \text{(E.32)} \\
&\overset{(c)}{\leq} \log_2\left(\mathbb{E}\|\mathcal{S}\|\right) && \text{(E.33)} \\
&\overset{(d)}{\leq} n\max\left\{0, I_1, I_2, I_3, I_4\right\} + \log_2(5)\ , && \text{(E.34)}
\end{aligned}$$

where (a) follows form the fact that $\mathcal{S}$ and $\|\mathcal{S}\|$ are functions of the output Z^n, the codebook and the chosen messages to be sent; (b) is a result of that knowing $\mathcal{E}=1$, the sent indices (S_0, S_1, S_2) belong to the set $\mathcal{S}$ and thus their uncertainty can not exceed the log cardinality of that set; and finally, (c) is a consequence of Jensen's inequality while (d) comes from (E.13) along with an application of the *log-sum-exp* inequality:

$$\log_2\left(\sum_{x\in\mathcal{X}} 2^x\right) \leq \max_{x\in\mathcal{X}} x + \log_2(\|\mathcal{X}\|)\ . \tag{E.35}$$

This, along with the previous remarks yields the following inequality:

$$\limsup_{n\to\infty} \frac{1}{n} H(S_0S_1S_2|Z^n\bar{W}_0\bar{W}_1\bar{W}_2, \mathcal{C}) \leq \max\left\{0, I_1, I_2, I_3, I_4\right\}\ . \tag{E.36}$$

E.3 Fourier-Motzkin Elimination

We resort to FME, recalling all the constraints:

$$T_1 \leq I(U_1;Y_1|Q) \ , \tag{E.37}$$
$$T_1 + T_0 \leq I(QU_1;Y_1) \ , \tag{E.38}$$
$$T_2 \leq I(U_2;Y_2|Q) \ , \tag{E.39}$$
$$T_2 + T_0 \leq I(QU_2;Y_2) \ , \tag{E.40}$$
$$T_0 - \bar{R}_0 \geq I(Q;Z) \ , \tag{E.41}$$
$$T_0 - \bar{R}_0 + T_1 - \bar{R}_1 \geq I(QU_1;Z) \ , \tag{E.42}$$
$$T_0 - \bar{R}_0 + T_2 - \bar{R}_2 \geq I(QU_2;Z) \ , \tag{E.43}$$
$$T_0 + T_1 + T_2 - (\bar{R}_0 + \bar{R}_1 + \bar{R}_2) \geq I(QU_1U_2;Z) + I(U_1;U_2|Q) \ , \tag{E.44}$$
$$T_1 - \bar{R}_1 - \tilde{R}_1 + T_2 - \bar{R}_2 - \tilde{R}_2 \geq I(U_1;U_2|Q) \ , \tag{E.45}$$
$$0 \leq \tilde{R}_1 \leq T_1 - \bar{R}_1 \ \ , \ \ 0 \leq \tilde{R}_2 \leq T_2 - \bar{R}_2 \ . \tag{E.46}$$

The resulting rate region after FME is as follows:

$$\bar{R}_1 \leq I(U_1;Y_1|Q) \ , \tag{E.47}$$
$$\bar{R}_1 + \bar{R}_0 \leq I(QU_1;Y_1) \ , \tag{E.48}$$
$$\bar{R}_2 \leq I(U_2;Y_2|Q) \ , \tag{E.49}$$
$$\bar{R}_2 + \bar{R}_0 \leq I(QU_2;Y_2) \ , \tag{E.50}$$
$$\bar{R}_1 + \bar{R}_2 \leq I(U_1;Y_1|Q) + I(U_2;Y_2|Q) - I(U_1;U_2|Q) \ , \tag{E.51}$$
$$\bar{R}_0 + \bar{R}_1 + \bar{R}_2 \leq I(QU_1;Y_1) + I(U_2;Y_2|Q) - I(QU_1U_2;Z) - I(U_1;U_2|Q) \ , \tag{E.52}$$
$$\bar{R}_0 + \bar{R}_1 + \bar{R}_2 \leq I(QU_2;Y_2) + I(U_1;Y_1|Q) - I(QU_1U_2;Z) - I(U_1;U_2|Q) \ , \tag{E.53}$$
$$\begin{aligned} 2\,\bar{R}_0 + \bar{R}_1 + \bar{R}_2 \leq\ & I(QU_2;Y_2) + I(QU_1;Y_1) \\ & - I(QU_1U_2;Z) - I(U_1;U_2|Q) - I(Q;Z) \ . \end{aligned} \tag{E.54}$$

Eliminating rate splitting parameters:

The achievable rate region writes then as:

$$R_1 - R_{01} \leq I(U_1;Y_1|Q) \ , \tag{E.55}$$
$$R_1 + R_{02} \leq I(QU_1;Y_1) \ , \tag{E.56}$$
$$R_2 - R_{02} \leq I(U_2;Y_2|Q) \ , \tag{E.57}$$
$$R_2 + R_{01} \leq I(QU_2;Y_2) \ , \tag{E.58}$$
$$R_1 - R_{01} + R_2 - R_{02} \leq I(U_1;Y_1|Q) + I(U_2;Y_2|Q) - I(U_1;U_2|Q) \ , \tag{E.59}$$
$$R_1 + R_2 \leq I(QU_1;Y_1) + I(U_2;Y_2|Q) - I(QU_1U_2;Z) - I(U_1;U_2|Q) \tag{E.60}$$
$$R_1 + R_2 \leq I(QU_2;Y_2) + I(U_1;Y_1|Q) - I(QU_1U_2;Z) - I(U_1;U_2|Q) \tag{E.61}$$
$$\begin{aligned} R_1 + R_2 + R_{01} + R_{02} \leq\ & I(QU_2;Y_2) + I(QU_1;Y_1) \\ & - I(QU_1U_2;Z) - I(U_1;U_2|Q) - I(Q;Z) \ . \end{aligned} \tag{E.62}$$

Eliminating the rates splitting parameters R_{01} and R_{02} with the positivity constrains: $R_{0,j} > 0$ and $R_j - R_{0j} > 0$ for $j \in \{1,2\}$, yields the desired inner bound.

E.4 Proof of Lemma 2

In this section, we show the convexity of the rate region given by:

$$\mathcal{R} : \begin{cases} R_1 & \leq & (1-e)\, h_2(x) + h_2(p) - h_2(p*x) \ , \\ R_2 & \leq & h_2(p*x) - h_2(p_2*x) \ . \end{cases} \tag{E.63}$$

where the union is over $x \in [0 : 0.5]$.

Obtaining this result comes to writing an equivalent of Mrs. Gerber's Lemma [61] in the presence of an eavesdropper in the same fashion as in [61]. Our aim will be to show that, for the corner point of this region, the rate R_2 is a concave function of the rate R_1.

Let us define the function f_1 as follows:

$$R_1 = f_1(x) \triangleq (1-e)h_2(x) + h_2(p) - h_2(p*x) \ . \tag{E.64}$$

We have that:

$$f_1'(x) = (1-e)h_2'(x) + (1-2p)h_2'(p*x) \ , \tag{E.65}$$

and,

$$f_1''(x) = (1-e)h_2''(x) + (1-2p)^2 h_2''(p*x) \ , \tag{E.66}$$

where:

$$h_2'(x) = \log_2\left(\frac{1-x}{x}\right) \qquad \text{and} \qquad h_2''(x) = -\frac{1}{x(1-x)} \ . \tag{E.67}$$

Let us also define the function f_2 as:

$$R_2 = f_2(x) \triangleq h_2(p_2*x) - h_2(p*x) \ . \tag{E.68}$$

In the same fashion, we can write:

$$f_2'(x) = (1-2p_2)h_2'(p_2*x) - (1-2p)h_2'(p*x) \ , \tag{E.69}$$

and

$$f_2''(x) = (1-2p_2)^2 h_2''(p_2*x) - (1-2p)^2 h_2''(p*x) \ . \tag{E.70}$$

To show that:

$$\frac{d^2R_2}{dR_1^2} = \frac{d^2f_2}{df_1^2} \leq 0 \ , \tag{E.71}$$

we observe that:

$$\frac{df_2}{df_1} = \frac{df_2}{dx}\frac{dx}{df_1} = \frac{df_2}{dx}\frac{df_1^{-1}(y)}{dy} = \frac{1}{f_1'(f_1^{-1}(y))}\frac{df_2}{dx} = \frac{1}{f_1'(x)}\frac{df_2}{dx} \ . \tag{E.72}$$

As such, one can write in the same manner that:

$$\frac{d^2f_2}{df_1^2} = \frac{f_2''(x)f_1'(x) - f_1''(x)f_2'(x)}{\left(f_1'(x)\right)^3} \ . \tag{E.73}$$

Since $0 \leq x \leq \frac{1}{2}$, then $0 \leq p*x \leq \frac{1}{2}$, and thus, one can easily check that:

$$f_1'(x) \geq 0 \ . \tag{E.74}$$

Thus, it suffices to show that for all $x \in [0 : 0.5]$,

$$f_2''(x)f_1'(x) - f_1''(x)f_2'(x) \leq 0 \ . \tag{E.75}$$

For notation convenience, we let:

$$a \triangleq 1 - 2p \qquad \text{and} \qquad a_2 \triangleq 1 - 2p_2 \ . \tag{E.76}$$

Now, one can write that:

$$\begin{aligned} f_2''(x)f_1'(x) - f_1''(x)f_2'(x) = a^2\, h_2''(p*x) \Big[(1-e)\, h_2'(x) - a_2\, h_2'(p_2 * x)\Big] \\ -a_2^2\, h_2''(p_2*x) \Big[(1-e)\, h_2'(x) - a\, h_2'(p*x)\Big] \\ -(1-e)\, h_2''(x) \Big[a\, h_2'(p*x) - a_2\, h_2'(p_2*x)\Big] \ , \end{aligned} \tag{E.77}$$

and thus

$$\begin{aligned} \frac{f_2''(x)f_1'(x) - f_1''(x)f_2'(x)}{h_2''(p*x)\, h_2''(p_2*x)\, h_2''(x)} = a^2\, \frac{(1-e)\, h_2'(x) - a_2\, h_2'(p_2*x)}{h_2''(p_2*x)\, h_2''(x)} - a_2^2\, \frac{(1-e)\, h_2'(x) - a\, h_2'(p*x)}{h_2''(p*x)\, h_2''(x)} \\ - (1-e)\, \frac{a\, h_2'(p*x) - a_2\, h_2'(p_2*x)}{h_2''(p_2*x) h_2''(p*x)} \ . \end{aligned} \tag{E.78}$$

Let us now define a variable α such that: $\alpha \triangleq 1 - 2x$. We have that:

$$a \cdot \alpha = 1 - 2(p*x) \qquad \text{and} \qquad a_2 \cdot \alpha = 1 - 2(p_2 * x) \ . \tag{E.79}$$

Moreover:

$$h_2'(x) = \log_2\left(\frac{1-x}{x}\right) = \log_2\left(\frac{1+\alpha}{1-\alpha}\right) \ , \tag{E.80}$$

$$h_2''(x) = -\frac{1}{x(1-x)} = -\frac{4}{1-\alpha^2} \ . \tag{E.81}$$

Then, to show the desired inequality (E.75), since:

$$h_2''(p*x)\, h_2''(p_2*x)\, h_2''(x) \leq 0 \ , \tag{E.82}$$

one only has to show, after some simplifications, that:

$$\begin{aligned} (1-e)\, \left(a^2 - a_2^2\right) \log_2\left(\frac{1+\alpha}{1-\alpha}\right) + a\, \left(1-(a\alpha)^2\right) \left[a_2^2 - 1 + e\left(1-(a_2\alpha)^2\right)\right] \log_2\left(\frac{1+a\alpha}{1-a\alpha}\right) \\ -a_2\, \left(1-(a_2\alpha)^2\right) \left[a^2 - 1 + e\left(1-(a\alpha)^2\right)\right] \log_2\left(\frac{1+a_2\alpha}{1-a_2\alpha}\right) \geq 0 \ . \end{aligned} \tag{E.83}$$

We will resort to the known series expansion of the log:

$$\log\left(\frac{1+\alpha}{1-\alpha}\right) = 2 \sum_{\substack{k=1 \\ k \text{ odd}}}^{\infty} \frac{\alpha^k}{k} \ , \tag{E.84}$$

to write that the inequality (E.83), after simplifications, requires:

$$(a_2^2 - a^2) \sum_{\substack{k=5 \\ k \text{ odd}}}^{\infty} \alpha^k \left[\left(\frac{1}{k-2} - \frac{1}{k} \right) T_k - \left(\frac{1}{k-4} - \frac{1}{k-2} \right) V_k \right] \geq -\frac{2}{3} \alpha^3 T_3 \ , \tag{E.85}$$

for all $\alpha \in [0:1]$, where

$$T_k = (1-e) \left(1 - \frac{a_2^{k+1} - a^{k+1}}{a_2^2 - a^2} \right) + a_2^2 \, a^2 \, \frac{a_2^{k-1} - a^{k-1}}{a_2^2 - a^2} \ , \tag{E.86}$$

$$V_k = e \, a_2^2 \, a_2 \, \frac{a_2^{k-3} - a^{k-3}}{a_2^2 - a^2} \ . \tag{E.87}$$

By hypothesis $p_2 \leq p$ and hence $a_2^2 - a^2 \geq 0$. We are thus left with only the analysis of the summation. In the sequel, we show the following results on summation operand.

Lemma 12 (Properties of some series)**.**

1. *The sequence $(T_k)_k$ dominates the sequence $(V_k)_k$ in that:*

$$(\forall k \in \mathbb{N}_{odd}) \ , \ T_k \geq V_k \geq 0 \ . \tag{E.88}$$

2. *If $a^2 + a_2^2 \leq 1$, then $(V_k)_{k \geq 5}$ for k odd is a decreasing sequence.*

3. *The following identity holds:*

$$-\frac{2}{3} \alpha^3 T_3 = \sum_{\substack{k=5 \\ k \ odd}}^{\infty} \alpha^3 T_3 \left(\frac{1}{k-2} - \frac{1}{k} - \frac{1}{k-4} + \frac{1}{k-2} \right) \ . \tag{E.89}$$

Proof: Proof is given in Appendix E.5. ■

Indeed, Lemma 12 motivates our choice $a^2 + a_2^2 \leq 1$ in the sequel and thus allows us to write:

$$\sum_{\substack{k=5 \\ k \text{ odd}}}^{\infty} \alpha^k \left[\left(\frac{1}{k-2} - \frac{1}{k} \right) T_k - \left(\frac{1}{k-4} - \frac{1}{k-2} \right) V_k \right] + \frac{2}{3} \alpha^3 T_3 \tag{E.90}$$

$$\overset{(a)}{=} \sum_{\substack{k=5 \\ k \text{ odd}}}^{\infty} \left(\frac{1}{k-2} - \frac{1}{k} \right) (\alpha^k T_k - \alpha^3 T_3) - \left(\frac{1}{k-4} - \frac{1}{k-2} \right) (\alpha^k V_k - \alpha^3 T_3) \tag{E.91}$$

$$\overset{(b)}{\geq} \sum_{\substack{k=5 \\ k \text{ odd}}}^{\infty} \left(\frac{1}{k-2} - \frac{1}{k} \right) (\alpha^k V_k - \alpha^3 T_3) - \left(\frac{1}{k-4} - \frac{1}{k-2} \right) (\alpha^k V_k - \alpha^3 T_3) \tag{E.92}$$

$$= \sum_{\substack{k=5 \\ k \text{ odd}}}^{\infty} \left(\frac{1}{k-2} - \frac{1}{k} - \frac{1}{k-4} + \frac{1}{k-2} \right) (\alpha^k V_k - \alpha^3 T_3) \tag{E.93}$$

$$\overset{(c)}{\geq} 0 \ , \tag{E.94}$$

where (a) comes from claim (3) in Lemma 12 and (b) results from claim (1) in Lemma 12 while (c) comes from the fact that

$$\frac{1}{k-2} - \frac{1}{k} - \frac{1}{k-4} + \frac{1}{k-2} \leq 0 \ , \tag{E.95}$$

and hence, since $(V_k)_{k\geq 5}$ is a decreasing sequence, then for all $\alpha \in [0:1]$ we can write that:

$$(\forall k \geq 5) \qquad \alpha^k V_k \leq \alpha^k V_5 \leq \alpha^3 V_5 \ , \tag{E.96}$$

and since:

$$T_3 - V_5 = (1-e)(1 - a^2 - a_2^2 + a^2\, a_2^2) \geq 0 \ , \tag{E.97}$$

then,

$$(\forall k \geq 5) \qquad \alpha^k V_k - \alpha^3 T_3 \leq 0 \ . \tag{E.98}$$

It is worth mentioning that the assumption $a_2^2 + a^2 \leq 1$ was used only in the monotony of the sequence (V_k).

E.5 Proof of Lemma 12

In this section, we prove the claims stated in Lemma 12. We start by showing claim (1) which consists to show that $\forall k \in \mathbb{N}_{\text{odd}}$, $T_k \geq V_k \geq 0$. Let the sequence $(S_k)_{k\in\mathbb{N}_{\text{odd}}}$ defined as follows:

$$S_k \triangleq \frac{a_2^{k-1} - a^{k-1}}{a_2^2 - a^2} \ , \tag{E.99}$$

with $k-1 \triangleq 2s$, then one can write that for all $k \geq 3$,

$$S_k = \sum_{j=0}^{s-1} a_2^{2\,j} a^{2\,(s-1-j)} \ . \tag{E.100}$$

Now, we know that:

$$T_k = (1-e)\,(1 - S_{k+2}) + a_2^2\, a^2\, S_k \ , \tag{E.101}$$

$$V_k = e\, a_2^2\, a_2\, S_{k-2} \ . \tag{E.102}$$

Let $k \geq 3$ for which we have that:

$$T_k - V_k = (1-e)\,(1 - S_{k+2}) + a_2^2\, a^2\, (S_k - e S_{k-2}) \ . \tag{E.103}$$

It is easy to check that:

$$S_k = a^{k-3} + a_2^2 S_{k-2} \ , \tag{E.104}$$

$$S_{k+2} = a_2^{k-1} + a^{k-1} + a^2\, a_2^2 S_{k-2} \ . \tag{E.105}$$

Thus, by substituting these expressions in (E.103), we end up with the next equality:

$$T_k - V_k = (1-e)\left(1 - a_2^{k-1} - a^{k-1}\right) + a_2^2\, a^2\, (S_k - S_{k-2}) \tag{E.106}$$

$$= (1-e)\left(1-a_2^{k-1}-a^{k-1}\right) + a_2^2\, a^2\left(a^{k-3} + (a_2^2-1)\, S_{k-2}\right) . \tag{E.107}$$

Now, from the choice of the system parameters (4.58), we see that:

$$\max\{a, a_2^2\} \leq 1-e \leq a_2 . \tag{E.108}$$

Then, to lower bound $T_k - V_k$ we split into the following cases:

- If $1 - a_2^{k-1} - a^{k-1} \geq 0$, then

$$\begin{aligned}
T_k - V_k &= (1-e)\left(1-a_2^{k-1}-a^{k-1}\right) + a_2^2\, a^2\left(a^{k-3} + (a_2^2-1)\, S_{k-2}\right) && \text{(E.109)}\\
&\geq a_2^2\left(1-a_2^{k-1}-a^{k-1}\right) + a_2^2\, a^2\left(a^{k-3} + (a_2^2-1)\, S_{k-2}\right) && \text{(E.110)}\\
&= a_2^2\left(1-a_2^{k-1} + (a_2^2-1)\, a^2\, S_{k-2}\right) && \text{(E.111)}\\
&= a_2^2(1-a_2^2)\left(\frac{1-a_2^{k-1}}{1-a_2^2} - a^2\, S_{k-2}\right) && \text{(E.112)}\\
&\overset{(a)}{=} a_2^2(1-a_2^2)\left(\sum_{j=0}^{s-1} a_2^{2\,j} - a^2 \sum_{j=0}^{s-2} a_2^{2\,j} a^{2\,(s-2-j)}\right) && \text{(E.113)}\\
&= a_2^2(1-a_2^2)\left(\sum_{j=0}^{s-1} a_2^{2\,j} - \sum_{j=0}^{s-2} a_2^{2\,j} a^{2\,(s-1-j)}\right) && \text{(E.114)}\\
&= a_2^2(1-a_2^2)\left(a_2^{k-3} + \sum_{j=0}^{s-2} a_2^{2\,j} \underbrace{\left(1-a^{2\,(s-1-j)}\right)}_{\geq 0}\right) && \text{(E.115)}\\
&\geq 0 . && \text{(E.116)}
\end{aligned}$$

  where (a) comes from (E.100) and some standard manipulations of multinomial coefficients.

- If $1 - a_2^{k-1} - a^{k-1} \leq 0$, then

$$\begin{aligned}
T_k - V_k &= (1-e)\left(1-a_2^{k-1}-a^{k-1}\right) + a_2^2\, a^2\left(a^{k-3} + (a_2^2-1)\, S_{k-2}\right) && \text{(E.117)}\\
&\geq \left(1-a_2^{k-1}-a^{k-1}\right) + a_2^2\, a^2\left(a^{k-3} + (a_2^2-1)\, S_{k-2}\right) && \text{(E.118)}\\
&= 1 - a_2^{k-1} - a^{k-1}(1-a_2^2) - a_2^2\, a^2(1-a_2^2)\, S_{k-2} && \text{(E.119)}\\
&= (1-a_2^2)\left(\frac{1-a_2^{k-1}}{1-a_2^2} - a^{k-1} - a_2^2\, a^2\, S_{k-2}\right) && \text{(E.120)}\\
&\overset{(a)}{\geq} (1-a_2^2)\left(\frac{1-a_2^{k-1}}{1-a_2^2} - a^{k-1} - a_2^4 S_{k-2}\right) && \text{(E.121)}\\
&= (1-a_2^2)\left(\sum_{j=0}^{s-1} a_2^{2\,j} - a^{k-1} - a_2^4 \sum_{j=0}^{s-2} a_2^{2\,j} a^{2\,(s-2-j)}\right) && \text{(E.122)}\\
&= (1-a_2^2)\left(\sum_{j=0}^{s-1} a_2^{2\,j} - a^{k-1} - \sum_{j=0}^{s-2} a_2^{2\,(j+2)} a^{2\,(s-2-j)}\right) && \text{(E.123)}
\end{aligned}$$

$$= (1-a_2^2)\left(\sum_{j=0}^{s-1} a_2^{2\,j} - a^{k-1} - \sum_{j=2}^{s} a_2^{2\,j} a^{2\,(s-j)}\right) \tag{E.124}$$

$$= (1-a_2^2)\left(\underbrace{1-a^{k-1}}_{\geq 0} + \underbrace{a_2^2 - a_2^{2\,s}}_{\geq 0} + \sum_{j=2}^{s-1} a_2^{2\,j}\left(1-a^{2\,(s-j)}\right)\right) \tag{E.125}$$

$$\geq 0\ , \tag{E.126}$$

where (a) comes from that $a_2 \geq a \geq 0$.

This proves our claim. Next, we show that if $a^2 + a_2^2 \leq 1$ then $(V_k)_{k\geq 5}$ is decreasing for k odd. Let k be an odd integer such that $k \geq 5$. We have that:

$$\frac{V_{k+2} - V_k}{e a^2 a_2^2} = S_{k+2} - S_k\ . \tag{E.127}$$

We check our last claim by induction, i.e., assuming $S_7 - S_5 \leq 0$ and

$$\forall k \geq 5\ ,\ S_{k+2} - S_k \leq 0 \qquad \text{then} \qquad S_{k+4} - S_{k+2} \leq 0\ .$$

To this end, we have that:

$$S_7 - S_5 = a_2^2(a^2 + a_2^2 - 1) \leq 0\ . \tag{E.128}$$

Let then $k \geq 5$, such that $S_{k+2} - S_k \leq 0$, thus:

$$S_{k+4} - S_{k+2} = a_2^{k+1} + (a^2-1)S_{k+2} \tag{E.129}$$

$$= a_2^{k+1} + (a^2-1)\left(a_2^{k-1} + a^2 S_k\right) \tag{E.130}$$

$$= a_2^{k+1} - a_2^{k-1} + a^2\left(a_2^{k-1} + (a^2-1)S_k\right) \tag{E.131}$$

$$= \underbrace{a_2^{k+1} - a_2^{k-1}}_{\leq 0} + a^2\ \underbrace{(S_{k+2} - S_k)}_{\leq 0} \tag{E.132}$$

$$\leq 0\ , \tag{E.133}$$

which proves the claim. Finally, it is easy to verify that:

$$-\frac{2}{3}\alpha^3 T_3 = \sum_{\substack{k=5 \\ k\ \text{odd}}}^{\infty} \alpha^3 T_3 \left(\frac{1}{k-2} - \frac{1}{k} - \frac{1}{k-4} + \frac{1}{k-2}\right)\ , \tag{E.134}$$

by noticing

$$\sum_{\substack{k=5 \\ k\ \text{odd}}}^{\infty} \left(\frac{1}{k-2} - \frac{1}{k} - \frac{1}{k-4} + \frac{1}{k-2}\right) = -\frac{2}{3}\ . \tag{E.135}$$

E.6 Proof of Theorem 42

In this section, we prove the result on the product of the two inversely less-noisy BC with a more-noisy eavesdropper.

E.6.1 Proof of the achievability

The achievability easily follows by evaluating the region:

$$\left\{\begin{array}{rcl} R_1 & \leq & I(QU_1;\mathbf{Y}) - I(QU_1;\mathbf{Z}) \ , \\ R_2 & \leq & I(QU_2;\mathbf{T}) - I(QU_2;\mathbf{Z}) \ , \\ R_1+R_2 & \leq & I(U_1;\mathbf{Y}|Q) + I(QU_2;\mathbf{T}) - I(QU_1U_2;\mathbf{Z}) - I(U_1;U_2|Q) \ , \\ R_1+R_2 & \leq & I(QU_1;\mathbf{Y}) + I(U_2;\mathbf{T}|Q) - I(QU_1U_2;\mathbf{Z}) - I(U_1;U_2|Q) \ , \\ R_1+R_2 & \leq & I(QU_1;\mathbf{Y}) - I(QU_1;\mathbf{Z}) + I(QU_2;\mathbf{T}) - I(QU_2;\mathbf{Z}) - I(U_1;U_2|\mathbf{Z}Q) \ , \end{array}\right. \tag{E.136}$$

based on the choices: $Q = (U_1, U_2)$ and $U_1 = X_1$ and $U_2 = X_2$ such that $P_{U_1X_1U_2X_2} = P_{U_1X_1}P_{U_2X_2}$.

The single rate constraints write thus as:

$$\begin{aligned} R_1 &\leq I(X_1;Y_1) - I(X_1;Z_1) + I(U_2;Y_2) - I(U_2;Z_2) && \text{(E.137)} \\ &\overset{(a)}{=} I(X_1;Y_1|Z_1) + I(U_2;Y_2) - I(U_2;Z_2) \ , && \text{(E.138)} \end{aligned}$$

where (a) is a result of that Z_1 is degraded towards Y_1. The sum-rates follow in a similar fashion, however the last sum-rate is redundant since:

$$I(X_1;X_2|Z_1Z_2U_1U_2) \leq I(X_1;X_2|U_1U_2) = 0 \ . \tag{E.139}$$

E.6.2 Proof of the converse

Let us concatenate the two outputs $\mathbf{Y} = (Y_1, Y_2)$, $\mathbf{Z} = (Z_1, Z_2)$ and $\mathbf{T} = (T_1, T_2)$. We start by single rate constraints.

Single-rate constraints

By Fano's inequality and the secrecy constraint, we have that:

$$\begin{aligned} n(R_1 - \epsilon_n) &\leq I(W_1;\mathbf{Y}^n) - I(W_1;\mathbf{Z}^n) && \text{(E.140)} \\ &\leq I(W_1;\mathbf{Y}^nZ_1^n) - I(W_1;\mathbf{Z}^n) && \text{(E.141)} \\ &= I(W_1;\mathbf{Y}^n|Z_1^n) - I(W_1;Z_2^n|Z_1^n) \ . && \text{(E.142)} \end{aligned}$$

Thus, by standard Csiszár & Körner's sum-identity (A.1) and some basic manipulations, we get that:

$$\begin{aligned} n(R_1 - \epsilon_n) &\leq \sum_{i=1}^{n} \Big[I(W_1;\mathbf{Y}_i|Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^n) - I(W_1;Z_{2,i}|Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^n) \Big] && \text{(E.143)} \\ &= \sum_{i=1}^{n} \Big[I(W_1;Y_{1,i}Y_{2,i}|Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^n) - I(W_1;Z_{2,i}|Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^n) \Big] && \text{(E.144)} \\ &= \sum_{i=1}^{n} \Big[I(W_1;Y_{2,i}|Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^n) - I(W_1;Z_{2,i}|Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^n) \\ &\qquad + I(W_1;Y_{1,i}|Y_{2,i}Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^n) \Big] && \text{(E.145)} \end{aligned}$$

$$\stackrel{(a)}{=} \sum_{i=1}^{n} \Big[I(W_1; Y_{2,i}|Z_{1,i}^n \mathbf{Y}^{i-1} Z_{2,i+1}^n) - I(W_1; Z_{2,i}|Z_{1,i}^n \mathbf{Y}^{i-1} Z_{2,i+1}^n) + I(W_1; Y_{1,i}|Y_{2,i} Z_{1,i}^n \mathbf{Y}^{i-1} Z_{2,i+1}^n) \Big] \tag{E.146}$$

$$\stackrel{(b)}{\leq} \sum_{i=1}^{n} \Big[I(W_1; Y_{2,i}|Z_{1,i}^n \mathbf{Y}^{i-1} Z_{2,i+1}^n) - I(W_1; Z_{2,i}|Z_{1,i}^n \mathbf{Y}^{i-1} Z_{2,i+1}^n) + I(X_{1,i}; Y_{1,i}|Z_{1,i})] \ , \tag{E.147}$$

where (a) follows from that Z_1 is degraded respect to Y_1 and (b) comes from the Markov chain:

$$(Z_1^{i-1}, \mathbf{Y}^{i-1}, Z_{2,i+1}^n, Y_{2,i}) \multimap X_{1,i} \multimap (Y_{1,i}, Z_{1,i}) \ . \tag{E.148}$$

Thus, letting $U_{2,i} = W_1$ and $V_2 = (Z_{1,i}^n, \mathbf{Y}^{i-1}, Z_{2,i+1}^n)$ we can simply get the rate constraint:

$$R_1 \leq I(X_1; Y_1|Z_1) + I(U_2; Y_2|V_2) - I(U_2; Z_2|V_2) \ . \tag{E.149}$$

Sum-rate constraint

We start by writing:

$$n(R_1 + R_2 - \epsilon_n) \leq I(W_1; \mathbf{Y}^n) - I(W_1; \mathbf{T}^n \mathbf{Z}^n) + I(W_1 W_2; \mathbf{T}^n \mathbf{Z}^n) \tag{E.150}$$

$$\leq I(W_1; \mathbf{Y}^n Z_1^n) - I(W_1; \mathbf{T}^n \mathbf{Z}^n) + I(W_1 W_2; \mathbf{T}^n \mathbf{Z}^n) \tag{E.151}$$

$$\stackrel{(a)}{=} I(W_1; \mathbf{Y}^n|Z_1^n) - I(W_1; \mathbf{T}^n Z_2^n|Z_1^n) + I(W_1 W_2; \mathbf{T}^n Z_2^n|Z_1^n) + n\epsilon_n \tag{E.152}$$

where (a) follows from the secrecy constraint. By standard manipulations, similarly to those used in the proof of the outer bound in Section 4.4.2, write that:

$$\begin{aligned} & n(R_1 + R_2 - \epsilon_n) \\ \leq & \sum_{i=1}^{n} \Big[I(W_1 \mathbf{T}_{i+1}^n; Y_i|Z_1^n \mathbf{Y}^{i-1} Z_{2,i+1}^n) - I(W_1 \mathbf{T}_{i+1}^n; \mathbf{T}_i Z_{2,i}|Z_1^n \mathbf{Y}^{i-1} Z_{2,i+1}^n) \\ & \qquad + I(W_1 W_2 \mathbf{T}_{i+1}^n Z_2^{i-1}; \mathbf{T}_i|Z_{2,i} Z_1^n \mathbf{Y}^{i-1} Z_{2,i+1}^n) \Big] \qquad \text{(E.153)} \\ = & \sum_{i=1}^{n} \Big[I(W_1 \mathbf{T}_{i+1}^n; Y_{1,i} Y_{2,i}|Z_1^n \mathbf{Y}^{i-1} Z_{2,i+1}^n) - I(W_1 \mathbf{T}_{i+1}^n; T_{1,i} T_{2,i} Z_{2,i}|Z_1^n \mathbf{Y}^{i-1} Z_{2,i+1}^n) \\ & \qquad + I(W_1 W_2 \mathbf{T}_{i+1}^n Z_2^{i-1}; T_{1,i} T_{2,i}|Z_{2,i} Z_1^n \mathbf{Y}^{i-1} Z_{2,i+1}^n) \Big] \qquad \text{(E.154)} \\ = & \sum_{i=1}^{n} \Big[I(W_1 \mathbf{T}_{i+1}^n; Y_{2,i}|Z_1^n \mathbf{Y}^{i-1} Z_{2,i+1}^n) - I(W_1 \mathbf{T}_{i+1}^n; T_{2,i} Z_{2,i}|Z_1^n \mathbf{Y}^{i-1} Z_{2,i+1}^n) \\ & \qquad + I(W_1 W_2 \mathbf{T}_{i+1}^n Z_2^{i-1}; T_{2,i}|Z_{2,i} Z_1^n \mathbf{Y}^{i-1} Z_{2,i+1}^n) \\ & \quad + I(W_1 \mathbf{T}_{i+1}^n; Y_{1,i}|Y_{2,i} Z_1^n \mathbf{Y}^{i-1} Z_{2,i+1}^n) - I(W_1 \mathbf{T}_{i+1}^n; T_{1,i}|T_{2,i} Z_{2,i} Z_1^n \mathbf{Y}^{i-1} Z_{2,i+1}^n) \\ & \qquad + I(W_1 W_2 \mathbf{T}_{i+1}^n Z_2^{i-1}; T_{1,i}|T_{2,i} Z_{2,i} Z_1^n \mathbf{Y}^{i-1} Z_{2,i+1}^n) \Big] \qquad \text{(E.155)} \\ \leq & \sum_{i=1}^{n} \Big[I(W_1 \mathbf{T}_{i+1}^n; Y_{2,i}|Z_1^n \mathbf{Y}^{i-1} Z_{2,i+1}^n) - I(W_1 \mathbf{T}_{i+1}^n; T_{2,i} Z_{2,i}|Z_1^n \mathbf{Y}^{i-1} Z_{2,i+1}^n) \\ & \qquad + I(X_{2,i}; T_{2,i}|Z_{2,i} Z_1^n \mathbf{Y}^{i-1} Z_{2,i+1}^n) \end{aligned}$$

$$+I(W_1\mathbf{T}_{i+1}^n;Y_{1,i}|Y_{2,i}Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^n)-I(W_1\mathbf{T}_{i+1}^n;T_{1,i}|T_{2,i}Z_{2,i}Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^n)$$
$$+I(W_1W_2\mathbf{T}_{i+1}^nZ_2^{i-1};T_{1,i}|T_{2,i}Z_{2,i}Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^n)\Big] \ . \tag{E.156}$$

On one hand, we observe that:

$$\begin{aligned}
&I(W_1\mathbf{T}_{i+1}^n;Y_{1,i}|Y_{2,i}Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^n)-I(W_1\mathbf{T}_{i+1}^n;T_{1,i}|T_{2,i}Z_{2,i}Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^n)\\
&\quad+I(W_1W_2\mathbf{T}_{i+1}^nZ_2^{i-1};T_{1,i}|T_{2,i}Z_{2,i}Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^n)\\
&=I(W_1\mathbf{T}_{i+1}^n;Y_{1,i}|Y_{2,i}Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^n)+I(W_2Z_2^{i-1};T_{1,i}|T_{2,i}Z_{2,i}Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^nW_1\mathbf{T}_{i+1}^n) &\text{(E.157)}\\
&\overset{(a)}{=}I(W_1\mathbf{T}_{i+1}^n;Y_{1,i}|Y_{2,i}Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^n)+I(W_2Z_2^{i-1};T_{1,i}|T_{2,i}Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^nW_1\mathbf{T}_{i+1}^n) &\text{(E.158)}\\
&\leq I(W_1\mathbf{T}_{i+1}^n;Y_{1,i}|Y_{2,i}Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^n)+I(X_{1,i};T_{1,i}|T_{2,i}Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^nW_1\mathbf{T}_{i+1}^n) \ , &\text{(E.159)}
\end{aligned}$$

where (a) follows from that Z_2 is degraded respect to T_2. On the other hand, we have that:

$$\begin{aligned}
I(X_{1,i};T_{1,i}|T_{2,i}Z_{1,i})&\overset{(a)}{=}I(X_{1,i};T_{1,i}|Z_{1,i})-I(T_{2,i};T_{1,i}|Z_{1,i}) &\text{(E.160)}\\
&\overset{(b)}{\leq}I(X_{1,i};T_{1,i}|Z_{1,i})-I(Y_{2,i};T_{1,i}|Z_{1,i}) &\text{(E.161)}\\
&=I(X_{1,i};T_{1,i}|Y_{2,i}Z_{1,i}) \ , &\text{(E.162)}
\end{aligned}$$

where (a) and (b) follow from the Markov chains:

$$(Y_{2,i},T_{2,i})\multimap X_{1,i}\multimap(Y_{1,i},Z_{1,i}) \qquad \text{and} \qquad (Y_{1,i},Z_{1,i})\multimap X_{2,i}\multimap(Y_{2,i},T_{2,i}) \ , \tag{E.163}$$

and thus this implies that T_2 is less-noisy than Y_2. From this observation, we have:

$$\begin{aligned}
&I(W_1\mathbf{T}_{i+1}^n;Y_{1,i}|Y_{2,i}Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^n)+I(X_{1,i};T_{1,i}|T_{2,i}Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^nW_1\mathbf{T}_{i+1}^n)\\
&\leq I(W_1\mathbf{T}_{i+1}^n;Y_{1,i}|Y_{2,i}Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^n)+I(X_{1,i};T_{1,i}|Y_{2,i}Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^nW_1\mathbf{T}_{i+1}^n) &\text{(E.164)}\\
&=I(X_{1,i};T_{1,i}|Y_{2,i}Z_1^n\mathbf{Y}^{i-1}Z_{2,i+1}^n) &\text{(E.165)}\\
&\leq I(X_{1,i};T_{1,i}|Z_{1,i}) \ . &\text{(E.166)}
\end{aligned}$$

Then, letting $S_{2,i}=\mathbf{T}_{i+1}^n$, the resulting sum-rate reads as:

$$R_1+R_2\leq I(X_1;Y_1|Z_1)+I(U_2S_2;Y_2|V_2)-I(U_2S_2;T_2Z_2|V_2)+I(X_2;T_2|Z_2V_2) \ . \tag{E.167}$$

The variable S_2 can be eliminated in a similar manner as we already did in Section 4.4.3. Since, Y_2 is less-noisy than Z_2 and so is T_1 towards Z_1, then we can show the converse of the region by letting $U_2\equiv(U_2,V_2)$ and $U_1\equiv(U_1,V_1)$.

Bibliography

[1] T. Cover, "Broadcast channels," *Information Theory, IEEE Transactions on*, vol. 18, no. 1, pp. 2–14, 1972.

[2] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975. [Online]. Available: http://dx.doi.org/10.1002/j.1538-7305.1975.tb02040.x

[3] K. Marton, "A coding theorem for the discrete memoryless broadcast channel," *Information Theory, IEEE Transactions on*, vol. 25, no. 3, pp. 306–311, 1979.

[4] P. Bergmans, "Random coding theorem for broadcast channels with degraded components," *Information Theory, IEEE Transactions on*, vol. 19, no. 2, pp. 197–207, 1973.

[5] H. Weingarten, Y. Steinberg, and S. Shamai, "The capacity region of the gaussian multiple-input multiple-output broadcast channel," *Information Theory, IEEE Transactions on*, vol. 52, no. 9, pp. 3936–3964, 2006.

[6] N. Devroye, P. Mitran, and V. Tarokh, "Achievable rates in cognitive radio channels," *Information Theory, IEEE Transactions on*, vol. 52, no. 5, pp. 1813–1827, 2006.

[7] I. Maric, R. Yates, and G. Kramer, "Capacity of interference channels with partial transmitter cooperation," *Information Theory, IEEE Transactions on*, vol. 53, no. 10, pp. 3536–3548, 2007.

[8] W. Wu, S. Vishwanath, and A. Arapostathis, "Capacity of a class of cognitive radio channels: Interference channels with degraded message sets," *Information Theory, IEEE Transactions on*, vol. 53, no. 11, pp. 4391–4399, 2007.

[9] C. E. Shannon, "Communication theory of secrecy systems*," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949. [Online]. Available: http://dx.doi.org/10.1002/j.1538-7305.1949.tb00928.x

[10] A. El Gamal, "The capacity of a class of broadcast channels," *Information Theory, IEEE Transactions on*, vol. 25, no. 2, pp. 166–169, 1979.

[11] M. S. P. S. I. Gel'fand, "Capacity of a broadcast channel with one deterministic component," *Probl. Peredachi Inf.*, vol. 16, pp. 24–34, 1980.

[12] A. El Gamal, "Capacity of the product and sum of two unmatched brodcast channels," *Probl. Peredachi Inf.*, vol. 16, pp. 3–23, 1980.

[13] M. Benammar and P. Piantanida, "On the role of interference decoding in compound broadcast channels," in *Information Theory Workshop (ITW), 2013 IEEE*, Sept 2013, pp. 1–5.

[14] F. Baccelli, A. El Gamal, and D. Tse, "Interference networks with point-to-point codes," *Information Theory, IEEE Transactions on*, vol. 57, no. 5, pp. 2582–2596, 2011.

[15] G. Caire and S. Shamai, "On the achievable throughput of a multiantenna gaussian broadcast channel," *Information Theory, IEEE Transactions on*, vol. 49, no. 7, pp. 1691–1706, 2003.

[16] M. H. M. Costa, "Writing on dirty paper (corresp.)," *Information Theory, IEEE Transactions on*, vol. 29, no. 3, pp. 439–441, 1983.

[17] A. Jovicic and P. Viswanath, "Cognitive radio: An information-theoretic perspective," *Information Theory, IEEE Transactions on*, vol. 55, no. 9, pp. 3945–3958, 2009.

[18] N. Liu, I. Maric, A. Goldsmith, and S. Shamai, "Bounds and capacity results for the cognitive z-interference channel," in *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*, 2009, pp. 2422–2426.

[19] M. Vaezi, "The capacity of less noisy cognitive interference channels," in *Communication, Control, and Computing (Allerton), 2012 50th Annual Allerton Conference on*, 2012, pp. 1769–1774.

[20] ——, "The capacity of more capable cognitive interference channels," *(available online) http://arxiv.org/abs/1207.2094*, 2014.

[21] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *Information Theory, IEEE Transactions on*, vol. 24, no. 3, pp. 339–348, 1978.

[22] E. Ekrem and S. Ulukus, "Secrecy capacity of a class of broadcast channels with an eavesdropper," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, pp. 824 235–, 2009. [Online]. Available: http://jwcn.eurasipjournals.com/content/2009/1/824235

[23] G. Bagherikaram, A. Motahari, and A. Khandani, "Secrecy capacity region of gaussian broadcast channel," in *Information Sciences and Systems. CISS 2009. 43rd Annual Conference on*, 2009, pp. 152–157.

[24] S. Shafiee and S. Ulukus, "Achievable rates in gaussian MISO channels with secrecy constraints," in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*, 2007, pp. 2466–2470.

[25] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379–423, 1948.

[26] S. Rini, D. Tuninetti, and N. Devroye, "New inner and outer bounds for the memoryless cognitive interference channel and some new capacity results," *Information Theory, IEEE Transactions on*, vol. 57, no. 7, pp. 4087–4109, 2011.

[27] T. Cover, "Comments on broadcast channels," *Information Theory, IEEE Transactions on*, vol. 44, no. 6, pp. 2524–2530, 1998.

[28] C. Nair and A. El Gamal, "An outer bound to the capacity region of the broadcast channel," in *Information Theory, 2006 IEEE International Symposium on*, 2006, pp. 2205–2209.

[29] C. Nair, "Capacity regions of two new classes of two-receiver broadcast channels," *Information Theory, IEEE Transactions on*, vol. 56, no. 9, pp. 4207–4214, 2010.

[30] B. Bandemer, A. Gamal, and Y.-H. Kim, "Simultaneous nonunique decoding is rate-optimal," in *Communication, Control, and Computing (Allerton), 2012 50th Annual Allerton Conference on*, 2012, pp. 9–16.

[31] S. Bidokhti and V. Prabhakaran, "Is non-unique decoding necessary?" *Information Theory, IEEE Transactions on*, vol. 60, no. 5, pp. 2594–2610, 2014.

[32] A. Padakandla and S. S. Pradhan, "A new coding theorem for three user discrete memoryless broadcast channel," *CoRR*, vol. abs/1207.3146, 2012.

[33] H. Weingarten, S. Shamai and G. Kramer, "On the compound MIMO broadcast channel," Information Theory and Applications (ITA 2007), UCSD, Palo-Alto, USA., Ed., Jan. 29-Feb. 2 2007.

[34] T. Gou, S. Jafar, and C. Wang, "On the degrees of freedom of finite state compound wireless networks," *Information Theory, IEEE Transactions on*, vol. 57, no. 6, pp. 3286–3308, 2011.

[35] M. Maddah-Ali, "On the degrees of freedom of the compound MISO broadcast channels with finite states," in *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, 2010, pp. 2273–2277.

[36] S. Jafar, *Interference Alignment: A New Look at Signal Dimensions in a Communication Network*. Now Publishers, 2011. [Online]. Available: http://books.google.fr/books?id=GfwB7ItK4esC

[37] C. Huang, S. Jafar, S. Shamai, and S. Vishwanath, "On degrees of freedom region of MIMO networks without channel state information at transmitters," *Information Theory, IEEE Trans. on*, vol. 58, no. 2, pp. 849 –857, feb. 2012.

[38] R. Tandon, S. Jafar, S. Shamai Shitz, and H. Poor, "On the synergistic benefits of alternating CSIT for the MISO broadcast channel," *Information Theory, IEEE Transactions on*, vol. 59, no. 7, pp. 4106–4128, 2013.

[39] H. Weingarten, T. Liu, S. Shamai, Y. Steinberg, and P. Viswanath, "The capacity region of the degraded multiple-input multiple-output compound broadcast channel," *Information Theory, IEEE Transactions on*, vol. 55, no. 11, pp. 5011–5023, 2009.

[40] H.-F. Chong and Y.-C. Liang, "The capacity region of a class of two-user degraded compound broadcast channels," in *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, 2013, pp. 932–936.

[41] P. Piantanida and S. Shamai, "On the capacity of compound state-dependent channels with states known at the transmitter," in *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, 2010, pp. 624–628.

[42] C. Nair and A. El Gamal, "The capacity region of a class of three-receiver broadcast channels with degraded message sets," *Information Theory, IEEE Transactions on*, vol. 55, no. 10, pp. 4479–4493, 2009.

[43] H. Witsenhausen and A. Wyner, "A conditional entropy bound for a pair of discrete random variables," *Information Theory, IEEE Transactions on*, vol. 21, no. 5, pp. 493–501, 1975.

[44] H. Eggleston, *Convexity*. Published by Cambridge University Press, 1958.

[45] S. Rini, D. Tuninetti, and N. Devroye, "Inner and outer bounds for the gaussian cognitive interference channel and new capacity results," *Information Theory, IEEE Transactions on*, vol. 58, no. 2, pp. 820–848, 2012.

[46] J. Jiang, I. Maric, A. Goldsmith, S. Shamai, and S. Cui, "On the capacity of a class of cognitive z-interference channels," in *Communications (ICC), 2011 IEEE International Conference on*, 2011, pp. 1–6.

[47] M. Vaezi and M. Vu, "On the capacity of the cognitive z-interference channel," in *Information Theory (CWIT), 2011 12th Canadian Workshop on*, 2011, pp. 30–33.

[48] C. Nair and Z. Wang, "The capacity region of the three receiver less noisy broadcast channel," *Information Theory, IEEE Transactions on*, vol. 57, no. 7, pp. 4058–4062, 2011.

[49] M. Vaezi, "Comments on "new inner and outer bounds for the memoryless cognitive interference channel and some new capacity results"," *Information Theory, IEEE Transactions on*, vol. 59, no. 6, pp. 4055–4056, 2013.

[50] O. Ozel and S. Ulukus, "Wiretap channels: Roles of rate splitting and channel prefixing," in *Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on*, 2011, pp. 628–632.

[51] Y. Liang and H. Poor, "Generalized multiple access channels with confidential messages," in *Information Theory, 2006 IEEE International Symposium on*, 2006, pp. 952–956.

[52] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Physical layer security in broadcast networks," *Security and Communication Networks, Wiley*, vol. 2, no. 5, pp. 227–238, 2009.

[53] R. Liu, I. Maric, P. S, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2493–2507, 2008.

[54] Y. Zhao, P. Xu, Y. Zhao, W. Wei, and Y. Tang, "Secret communications over semi-deterministic broadcast channels," in *Communications and Networking in China, 2009. ChinaCOM 2009. Fourth International Conference on*, 2009, pp. 1–4.

[55] W. Kang and N. Liu, "The secrecy capacity of the semi-deterministic broadcast channel," in *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*, 2009, pp. 2767–2771.

[56] R. Liu and H. Poor, "Secrecy capacity region of a multiple-antenna gaussian broadcast channel with confidential messages," *Information Theory, IEEE Transactions on*, vol. 55, no. 3, pp. 1235–1249, 2009.

[57] R. Liu, T. Liu, H. Poor, and S. Shamai, "Multiple-input multiple-output gaussian broadcast channels with confidential messages," *Information Theory, IEEE Transactions on*, vol. 56, no. 9, pp. 4215–4227, 2010.

[58] E. Ekrem and S. Ulukus, "The secrecy capacity region of the gaussian mimo multi-receiver wiretap channel," *Information Theory, IEEE Transactions on*, vol. 57, no. 4, pp. 2083–2114, 2011.

[59] Y. Liang, H. V. Poor, and S. Shamai (Shitz), *Information Theoretic Security*. Foundations and Trends in Communications and Information Theory, Now Publishers, Hanover, MA, USA, 2008, vol. 5, no. 4-5.

[60] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: A summary of recent advances," *Signal Processing Magazine, IEEE*, vol. 30, no. 5, pp. 16–28, 2013.

[61] A. Wyner and J. Ziv, "A theorem on the entropy of certain binary sequences and applications–i," *Information Theory, IEEE Transactions on*, vol. 19, no. 6, pp. 769–772, 1973.

[62] Y. Geng, A. Gohari, C. Nair, and Y. Yu, "The capacity region for two classes of product broadcast channels," in *Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on*, 2011, pp. 1544–1548.

[63] T. Cover and J. Thomas, *Elements of information theory (2nd Ed)*. Wiley-Interscience, 2006.

[64] A. Gohari and V. Anantharam, "Evaluation of marton's inner bound for the general broadcast channel," *Information Theory, IEEE Transactions on*, vol. 58, no. 2, pp. 608–619, 2012.

[65] A. Gohari, C. Nair, and V. Anantharam, "On Marton's inner bound for broadcast channels," in *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, July 2012, pp. 581 –585.

[66] V. Jog and C. Nair, "An information inequality for the bssc broadcast channel," in *Information Theory and Applications Workshop (ITA), 2010*, 2010, pp. 1–8.

[67] Y. Liang, G. Kramer, and H. Poor, "Equivalence of two inner bounds on the capacity region of the broadcast channel," in *Communication, Control, and Computing, 2008 46th Annual Allerton Conference on*, 2008, pp. 1417–1421.

[68] C. Nair, "An achievable rate region for the 2-receiver broadcast channel obtained by viewing it as an interference channel," in *Wireless Communications & Signal Processing, 2009. WCSP 2009. International Conference on*, 2009, pp. 1–5.

[69] J. Villard, "Fourrier motzking gui," online at "http://www.joffrey-villard.fr/FMG.php?lang=en".

[70] Y. Liang, G. Kramer, H. Poor, and S. (Shitz), "Compound wiretap channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, pp. 142 374–, 2009. [Online]. Available: http://jwcn.eurasipjournals.com/content/2009/1/142374

[71] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2453–2469, 2008.

[72] I. Csiszar and J. Körner, *Information theory: coding theorems for discrete memoryless systems*. Akadémiai Kiado, Budapest, 1982.